

5. Corporate Governance

Management Approach

5.1 About Wistron

- 5.1.1 Company Profile
- 5.1.2 Products and Services

5.2 Corporate Governance

- 5.2.1 Functions of Board of Directors
- 5.2.2 Ethical Management
- 5.2.3 Legal Compliance

5.3 Risk Management

- 5.3.1 Enterprise Risk Management
- 5.3.2 Information Security/Cybersecurity & Privacy Protection
- 5.3.3 Intellectual Property Rights Management Policy

5.4 Moving Towards a Sustainable Supply Chain

- 5.4.1 Supply Chain Management Framework and Overview
- 5.4.2 Supply Chain Sustainability Management
- 5.4.3 Conflict Minerals Management

5.5 Operating Capability

- 5.5.1 Financial Performance
- 5.5.2 Tax Policy
- 5.5.3 Policy Impact



Black-faced Spoonbill

The black-faced spoonbill is the most endangered migratory bird among the six species of spoonbills in the world and was internationally classified as an endangered species. Every year in September and October, over 60% of the global population of Black-faced Spoonbills flies to Taiwan to spend the winter, staying until they begin their northward migration in March or April of the following year. Wistron enhances public awareness and support for ecological protection through long-term conservation efforts.





Management Approach

● above 95% ● 90%–95% ● below 90%

Topic	Strategy	2024 Targets	2024 Results	Status	2025 Targets	2030 Targets
Corporate Governance & Ethical Management	Improve performance in global sustainability assessment	1. Maintain a top-tier ranking in the top 5% among listed companies in the Corporate Governance Evaluation 2. Maintained strong performance in ESG ratings 3. Achieve at least 20% representation of directors of different genders on the Board 4. Link executive officer compensation to ESG performance indicators 5. Increase the attendance rate of individual directors at each term to 80%	1. Ranked in the top 5% of listed companies in the Corporate Governance Evaluation 2. Maintained strong performance in ESG ratings 3. Achieved 20% female representation on the Board 4. Established linkage between executive officer compensation and ESG performance indicators 5. All directors achieved an individual attendance rate of 80% or above in 2024	●	1. Maintain a top-tier ranking (top 5% among listed companies) in the Corporate Governance Evaluation 2. Maintain or improve strong performance in ESG ratings 3. Achieve at least 20% representation of directors of different genders on the Board 4. Link executive compensation to ESG performance indicators 5. Ensure individual director attendance rates reach at least 80% per term	1. Maintain a top-tier ranking in the top 5% among listed companies in the Corporate Governance Evaluation 2. Maintain or improve the ESG ratings and performance 3. Achieve at least 20% representation of directors of different genders on the Board 4. Link executive compensation to ESG performance indicators 5. Ensure individual director attendance rates reach at least 80% per term
	Implement employee training to strengthen the Code of Conduct and foster a culture of integrity and ethical business practices	Achieve a 100% signing rate of Code of Conduct Statement	100%	●	100%	100%
Risk and Crisis Management	Regularly identify the risk appetite for all levels of the Company	1. Establish a comprehensive enterprise risk management system and submit an annual risk report to the Board of Directors 2. No material risk events involving amounts over NT\$100 million occurred under the enterprise risk management system.	1 case (See Section 4.4.2 Occupational Safety and Health – Incident Investigation for details.)	●	1. Systematize risk surveys and the risk database 2. Strengthen the company's business contingency plan in response to geopolitical risk threats 3. Conduct risk sensitivity analyses and stress testing 4. Continuously manage and mitigate the probability of significant risks occurring to the company (The significant risks are defined by property loss exceeding NT\$100 million)	Continuing to manage and mitigate the probability of significant risks occurring to the company. (The significant risks are defined by property loss exceeding NT\$100 million)
		Conduct regular self-assessments of internal controls and achieve a reliability coefficient ≥ 95%	ICS (Internal Controls Self-assessment): 99.95% (1H) 99.95% (2H) ICE (Internal Controls Evaluation): 99.97%	●	Conduct regular self-assessments of internal controls and achieve a reliability coefficient ≥ 95%	Conduct regular self-assessments of internal controls and achieve a reliability coefficient ≥ 95%
Corporate Governance & Ethical Management	Establish a regulatory compliance system and regularly review domestic and international regulatory changes relevant to operations to ensure all business activities comply with applicable laws and regulations	Employees : No material violations of laws (fines exceeding NT\$1,000,000)	Employees : No material violations of laws (fines exceeding NT\$1,000,000)	●	Employees : No material violations of laws (fines exceeding NT\$1,000,000)	Employees : No material violations of laws (fines exceeding NT\$1,000,000)



Management Approach

● above 95% ● 90%–95% ● below 90%

Topic	Strategy	2024 Targets	2024 Results	Status	2025 Targets	2030 Targets
		Shareholder / Securities Related Matters 1. Compliant with regulations and free of penalties 2. Closely monitor regulatory or policy changes issued by competent authorities and adjust internal management practices accordingly	Shareholder / Securities Related Matters 1. Complied with all regulations without incurring any penalties 2. Closely monitored regulatory and policy changes issued by competent authorities and adjusted internal management practices accordingly. 3. Completed compliance training for all internal managers	●	Shareholder / Securities Related Matters 1. Compliant with regulations and free of penalties 2. Closely monitor regulatory or policy changes issued by competent authorities and adjust internal management practices accordingly 3. Regulatory compliance training for all internal managers	Shareholder / Securities Related Matters 1. Compliant with regulations and free of penalties 2. Closely monitor regulatory or policy changes issued by competent authorities and adjust internal management practices accordingly
		Environmental Health and Safety 1.Stay up to date with regulatory developments, remain compliant, and incur no major penalties (fines exceeding NT\$1 million) 2. Regularly conduct EHS (Environment, Health, and Safety) regulatory identification and timely adjust internal procedures accordingly.	1. Stayed up to date with regulations, ensured compliance, and incurred no material penalties (fines exceeding NT\$1 million) 2. Regularly identified applicable EHS (Environmental, Health, and Safety) regulations and adjusted internal company procedures accordingly	●	Environmental Health and Safety 1. Stayed up to date with regulatory developments, remained compliant, and incurred no material penalties (fines exceeding NT\$1 million) 2. Regularly conducted EHS (Environment, Health, and Safety) regulatory identification and timely adjusted internal procedures accordingly	Environmental Health and Safety 1. Stayed up to date with regulations, ensured compliance, and incurred no material penalties (fines exceeding NT\$1 million) 2. Regularly identified applicable EHS (Environmental, Health, and Safety) regulations and adjusted internal company procedures accordingly
		Customer / Supplier / Litigation / Patent / Trademark Achieve 95% digitalization of contract and intellectual property asset management; continuously monitor international regulatory trends and customer needs to respond and adapt accordingly.	Customer / Supplier / Litigation / Patent / Trademark contract and intellectual property asset management digitalization reached 93.7%	●	Customer / Supplier / Litigation / Patent / Trademark Achieve 95% digitalization of contract and intellectual property asset management; continuously monitor international regulatory trends and customer needs to respond and adapt accordingly.	In addition to the digitalization of contracts and intellectual property asset management, as well as the continuous monitoring of international regulatory trends and customer needs for timely responses and adjustments, big data analytics will also be applied to the database to serve as a strategic reference for future planning.
Information Security/ Cybersecurity & Privacy	Establish an updated information security/cybersecurity system and mechanism to ensure information security for the company and its customers	The facility passed the customer assessment on information security/cybersecurity compliance. Certification rate: 100%	100%	●	100%	100%
		100% of the facility has obtained ISO/IEC 27001 certification coverage	100%	●	The headquarters office and all manufacturing facilities have achieved 100% ISO/IEC 27001 certification and continue to maintain their validity through regular updates	The headquarters office and all manufacturing facilities have achieved 100% ISO/IEC 27001 certification and continue to maintain their validity through regular updates



Management Approach

● above 95% ● 90%–95% ● below 90%

Topic	Strategy	2024 Targets	2024 Results	Status	2025 Targets	2030 Targets
Supplier Sustainability Management	Strengthen Supply Chain Sustainable Resilience	Risk identification 1. Tier 1 suppliers' compliance rate 100% 2. Critical non-tier 1 suppliers' compliance rate > 100%	1.100% 2.100%	<div></div>	1.100% 2.100%	1.100% 2.100%
		Ratio of sustainability audit on high-risk suppliers = 100%	100%	<div></div>	100%	100%
		Improvement and guidance of audit deficiency for high-risk suppliers NCR completion rate: 100%	100%	<div></div>	100%	100%
	Deepen Regional & Strategic Cooperation*	Machinery and materials in the China Site > 98%	98.06%	<div></div>	> 98%	> 98%
		Machinery and materials in the Vietnam site > 50%	54.66%	<div></div>	> 55%	> 70%
	Signature of Major Statements	100% Declaration signing rate of the code of conduct for tier 1 suppliers	100%	<div></div>	100%	100%
		100% Declaration signing rate of the "Declaration of Non-use of Conflict Minerals"	100%	<div></div>	100%	100%
	Optimize Strategy Supplier Core Competitiveness	Greenhouse gas reduction and water source inventory coverage > 67%	85%	<div></div>	Coverage > 67%	Coverage > 85%
		Suppliers with high energy consuming material obtaining GHG external verification (ISO 14064-1) ≥ 70%	75%	<div></div>	≥ 75%	≥ 85%
		Suppliers with high energy consuming material obtaining energy management system external verification (ISO 50001) ≥ 60%	65.38%	<div></div>	≥ 65%	≥ 70%
Note : *Optimize regional supply chain: The proportion of local procurement is based on the major manufacturing sites of Wistron's key operational locations, which include five major sites in China and one major site in Vietnam, using suppliers from the local regions.						

5.1 About Wistron

5.1.1 Company Profile

Global Leader in the ICT Industry

Wistron Corporation is a leading global technology service provider supplying innovative ICT (information and communications technology) products, service solutions, and systems to top-tier global brands. In recent years, Wistron has driven growth through its strong R&D and technological innovation capabilities, as well as diversified product development. In addition to portable computers, desktop systems, servers, and enterprise storage devices, Wistron offers professional display products, communication devices, and after-sales services. The company has also embraced the trend of cloud computing by tightly integrating hardware, such as computers and smart devices, with cloud-based data systems through software services. This integration enables the delivery of technical service platforms and comprehensive solutions. Wistron is also actively building new technology value chains and innovation platforms, and the scope of technologies now extends further to include emerging fields such as AI, 5G, metaverse-related applications, in-vehicle systems, and Industry 4.0 automation, among others. The Company is committed to realizing its vision of “Sustainability through Innovation.”

Global Operations

Headquartered in Taiwan, Wistron has established a global footprint with logistics and operational sites across the Asia-Pacific, Europe, and the Americas. The Company employs over 45,000 people worldwide, operating ten manufacturing facilities, eleven R&D and technical support centers, and thirteen customer service centers. The total area of its major manufacturing sites spans approximately 2,525,000 square meters (based on 1,000 m² units). In response to the needs of global brand clients and dynamic markets, Wistron leverages the unique strengths of each region to deliver tailored, end-to-end product and service solutions, ensuring strong product development capabilities and comprehensive customer support. Through the coordinated efforts of professional teams at Wistron's Taiwan operations and R&D headquarters, as well as its overseas sites, the Company has achieved steady growth and demonstrated strong operational performance. For more information on Wistron's global operations, please visit [Wistron's official website](#).

Note: Some sites have multiple functions





5.1.2 Products and Services

Driven by growth from diversified ICT product development, Wistron has not only continued to deliver environmentally friendly, high-value-added products but has also accelerated its transformation into a comprehensive Technology Service Provider (TSP). As part of this transition, the Company offers innovative design, manufacturing, services, and systems focused on information and communications technology. In line with the development of cloud technologies, Wistron seamlessly integrates hardware, such as computers and smart devices, with cloud-based data systems through software services. This enables the provision of technical service platforms and solutions that are precisely tailored to the evolving needs of customers and end users.


Main Products and Technology Services

Wistron’s revenue is primarily derived from the manufacturing of 3C (computer, communication, and consumer electronics) products. In addition to actively securing orders from major international brands, the Company recognizes that effective cost control and maintaining stable gross margins are critical factors for competitiveness in an increasingly price-sensitive market. In 2024, Wistron saw notable growth in AI computing devices and large-scale data center products, while other product lines remained stable or experienced slight declines.






Notebook computers, desktop computers, all-in-one PCs, monitors, and VoIP phones



AI Computing devices, Switch & Network Security Devices, industrial PCs, smartphones & handheld mobile devices, and after-sales services



Green recycling services, display components, and digital signage

Production Volume in the Past Two Years


Unit: thousand units/panels/pieces


Year	2023	2024
3C products	64,854	65,426
Other products	12,127	3,430
Total	76,981	68,856





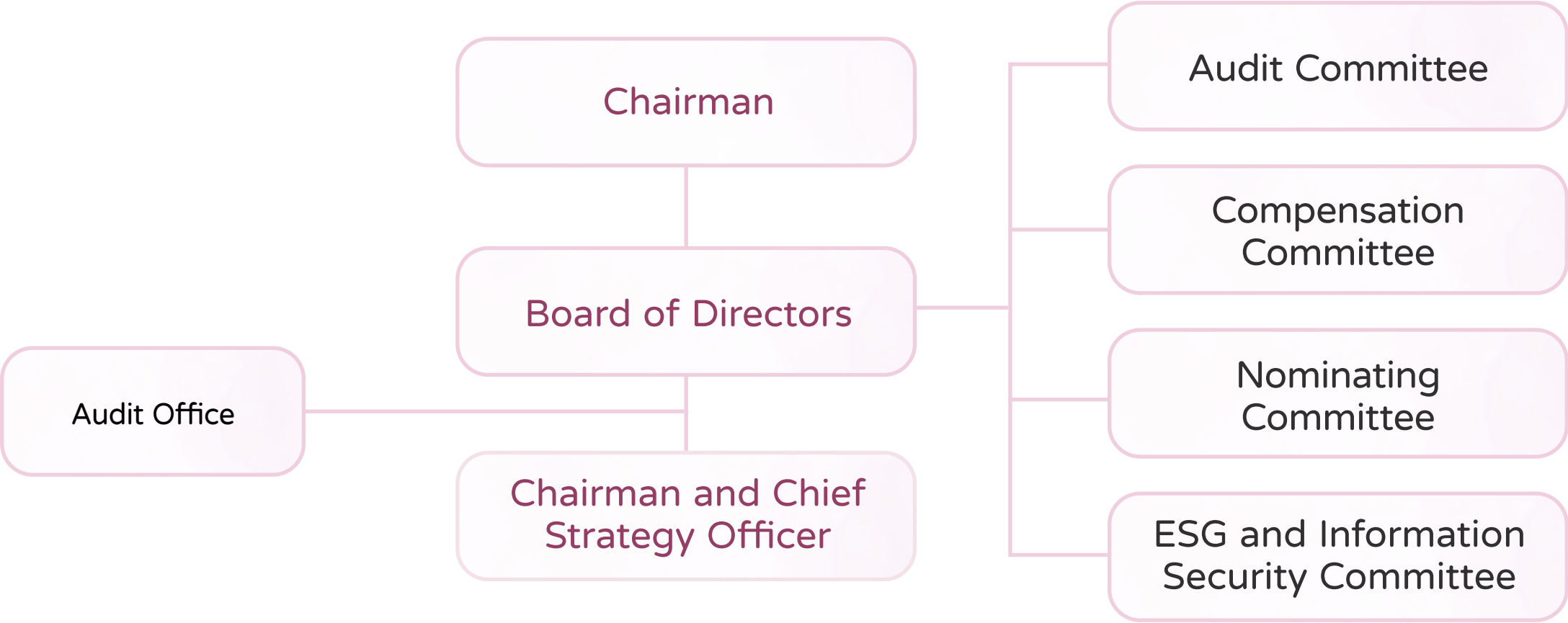
5.2 Corporate Governance

 **Top 5 % in Corporate Governance Evaluation**

 **Taiwan Corporate Governance 100 Index constituent stock**

Wistron believes that sound corporate governance is the foundation of sustainable business development. The Company is committed to establishing an effective governance framework based on principles of protecting shareholder rights, strengthening Board functions, respecting stakeholder interests, and enhancing information transparency. In accordance with Article 277 of the Company Act, amendments to the Articles of Incorporation must be approved by shareholders at a general meeting, ensuring their participation in major corporate decisions. The scope of directors’ responsibilities is not subject to limitation, as stipulated by relevant provisions of the Company Act. Wistron continuously implements various policies and mechanisms to enhance governance quality, with the aim of maximizing shareholder value and ensuring sustainable corporate operations.

5.2.1 Functions of Board of Directors



The Board of Directors serves as Wistron’s highest governing body, responsible for overseeing the management team to ensure compliance with applicable laws and regulations while enhancing information transparency. Leveraging their professional expertise, board members provide strategic guidance on major decisions to prevent the implementation of policies that could undermine the Company’s value. They also emphasize the cultivation of a culture rooted in integrity and ethical conduct, fulfilling corporate responsibilities to support sustainable operations and protect shareholder interests. The management team also regularly reports to the Board of Directors on the Company’s operational status, development strategies, and sustainability-related matters, including updates on sustainability initiatives and progress, the implementation of ethical business practices, information security and cybersecurity measures, material topics, and stakeholder engagement. This ensures smooth and effective communication between the management team and the Board. In compliance with governance guidelines, the Board of Directors convenes at least once per quarter and held a total of ten meetings in 2024. The average attendance rate among board members reached 99%, surpassing Wistron’s requirement of an annual attendance rate of at least 80%.





Functional Committee

To strengthen the Board’s supervisory function and enhance management effectiveness, Wistron has established four functional committees under the Board: the Audit Committee, the Compensation Committee, the Nominating Committee, and the ESG and Information Security Committee (formerly the ESG Committee). The operational status of each functional committee is detailed in the table below. For further information, please refer to Wistron's [Annual Report](#).

Committee	Function	Members	Attendance rate (excl. proxy)	Major Resolutions
Audit Committee	Oversees the fair presentation of Wistron’s financial statements; the appointment, dismissal, independence, and performance of certified public accountants; the effective implementation of internal controls; compliance with applicable laws and regulations; and the management of existing or potential risks.	Independent Director Mr. Chien-Hsin Chuang, Independent Director Mr. Jack Chen, Independent Director Mr. S.J. Paul Chien, Independent Director Ms. Pei-Pei Yu, Independent Director Ms. Mei-Ling Chen	100%	<ul style="list-style-type: none">• Annual & quarterly financial statements• Major investment projects• Major loans, endorsements & guarantees• Risk management reports
Compensation Committee	Establishes and periodically reviews policies, systems, standards, and structures for the performance evaluation and compensation of directors and managers, and regularly evaluates and determines their compensation.	Independent Director Mr. S.J. Paul Chien, Independent Director Mr. Jack Chen, Independent Director Ms. Pei-Pei Yu	100%	<ul style="list-style-type: none">• Recommendations on director remunerations• Recommendations on performance bonuses & salary adjustments for managers• Recommendation on Employee Compensation for Managers
Nominating Committee	Selects and reviews qualified candidates for directors, managers, and members of Board committees, and establishes and periodically reviews the structure and functioning of Board committees.	Independent Director Ms. Pei-Pei Yu, Chairman Mr. Simon Lin, Independent Director Mr. Jack Chen, Independent Director Ms. Mei-Ling Chen	100%	<ul style="list-style-type: none">• Nominated Board candidates• Organized training for directors
ESG and Information Security Committee	Formulates the direction and objectives for corporate social responsibility, sustainability, and information security/cybersecurity, and oversees related policies, implementation plans, and performance.	Director, President & CEO Mr. Jeff Lin, Director Philip Peng, Independent Director Ms. Mei-Ling Chen,	91% *	<ul style="list-style-type: none">• Reviewed progress to sustainability targets & set future goals• Established Wistron's "Sustainable Materials Policy," "Sustainable Procurement Policy" & "Nature and Biodiversity & No Deforestation Policy"• Amended Wistron's "Code of Conduct," "Environmental Policy," "ESG & Information Security Committee Charter" & "Sustainable Development Best Practice Principles"• Reported on material sustainability topics and stakeholder communication• Reported on the implementation of integrity management and information security/cybersecurity• Presented the progress of subsidiaries’ greenhouse gas inventory and verification schedule

Note: On April 2, 2025, the Company’s ESG Committee was renamed to ESG and Information Security Committee. The composition of committee members was also revised, replacing senior executives and independent directors with board members, and requiring the participation of at least one independent director.



Composition and Diversity of the Board of Directors

In accordance with the [Articles of Incorporation](#), the Company shall have seven to nine directors, each serving a three-year term. A candidate nomination system is adopted, and directors are elected by the shareholders' meeting from a list of nominated candidates to safeguard shareholders' rights and interests. The Company has stipulated a Board diversity policy in Article 20 of its [Corporate Governance Best Practice Principles](#), stating that the composition of the Board should consider multiple aspects, including gender, nationality, culture, professional background, and industry experience. For specific management objectives and progress regarding board member diversity, please visit our [website](#).

Wistron's Board of Directors currently consists of nine members, all of whom are highly respected professionals with extensive experience in the industry. Following the re-election upon the expiration of their term in 2024, the average tenure is eight years. Two members (22%) also serve as company executives, and five seats (approximately 56%) are held by independent directors, all of whom meet the independence requirements set forth in the "Regulations Governing Appointment of Independent Directors and Compliance Matters for Public Companies." The Board also includes two female directors, accounting for approximately 22%. For information on the procedures related to the election of Board members, please visit the company's [website](#). In addition, none of the Company's directors concurrently serve as directors at more than four other public companies. Comprehensive information on each Board member—including educational and professional background, concurrent positions in other companies, attendance records, and other relevant details—is disclosed in the Company's annual report and on its official website.

The Chairperson of the Board is elected by the Board of Directors and serves as the leader of the Board internally and the Company's representative externally. To uphold the Board's intent and enhance

decision-making efficiency, the Chairperson also serves as the Chief Strategy Officer, responsible for strategic planning, development, implementation, and long-term corporate growth. In the event of any proposals involving conflicts of interest, the Chairperson abstains from participation in accordance with the principle of avoidance.

Director Training and Performance Evaluation of the Board of Directors

To enhance directors' knowledge and competencies in areas such as regulations, economics, environment, social issues, and risk management, the Company arranges annual training courses for Board members. In 2024, the training topics included: "AI and the Open Source ERA-Navigating Corporate Legal Risks", which explored the legal risks enterprises may face with the rise of AI and the trends in international regulations; and "Building Sustainable Competitiveness through DEI", which covered the meaning and spirit of DEI (Diversity, Equity, and Inclusion), and strategies for integrating DEI into internal corporate practices. Each director completed an average of 10.3 hours of training in 2024. In addition, to ensure regulatory compliance, the Company also provided an online training course on insider trading prevention regulations for all directors and managers.

To ensure effective corporate governance and enhance the performance of the Board of Directors, Wistron conducts annual performance evaluations of the Board and its functional committees in accordance with the "Rules for Board of Directors and Function Committee Performance Assessments ". These evaluations encompass key areas, including legal compliance, corporate governance, risk management, and sustainable development goals, to ensure that the Board and its committees fulfill their responsibilities across all ESG dimensions. The evaluation results serve as a basis for determining compensation and for the continuous enhancement of the Board's operations and effectiveness. In 2024, performance evaluations were conducted for the Board of Directors, Audit Committee, Compensation Committee, Nominating Committee,

and ESG and Information Security Committee (formerly ESG Committee). Upon completion of the scoring and analysis, the performance evaluation scores for the Board of Directors and its functional committees were 99.56, 99.60, 100, 100, and 99.86, respectively. All results were rated as "Exceeds Standards" and have been reported to the Board and each respective committee. In addition, the Company commissions an external professional independent organization or team of external experts and scholars to conduct a Board performance evaluation at least once every three years. In 2022, the Company engaged the Corporate Governance Association to carry out an external evaluation of the Board. The results provided positive affirmation regarding the Board structure, meeting dynamics, training arrangements, and various aspects of ESG development. The next external performance evaluation is scheduled to be conducted in the fourth quarter of 2025. For detailed information on the Company's director training and Board performance evaluation reports, please refer to the [Company's annual report](#) and official [website](#).





Conflicts of interest Management

For agenda items that may involve conflicts of interest for Directors or the legal entities they represent, compliance with Article 15 of the Rules and Procedures of Board of Directors Meetings is required. In such instances, Directors must disclose the relevant details of the conflict during the meeting. If their participation in discussions or voting may compromise the Company’s interests, they are required to abstain and recuse themselves. Additionally, they are prohibited from exercising voting rights on behalf of other Directors. If a director’s spouse, relatives within the second degree of kinship, or a company under the Director’s control has a vested interest in the meeting agendas, the Director is considered to have a personal interest in the matter.

For details on the execution of director recusals from conflict-of-interest agenda items in 2024, concurrent directorships held by Board members, cross-shareholdings with suppliers or other stakeholders, the existence of controlling shareholders, and information on related parties, their relationships, transactions, and outstanding balances, please refer to the [Company’s annual report](#).

Compensation Policy for the Board of Directors and Senior Executives

The compensation for the Company’s directors includes remuneration and business execution expenses. In accordance with Articles 11 and 16 of the Articles of Incorporation, director remuneration is allocated from an amount not exceeding 1% of the Company’s annual profit. Reasonable compensation is granted based on the Company’s operating results and the individual director’s contribution. All payments are made in accordance with the Guidelines for Director and Functional Committee Remuneration and are subject to prior approval by the Compensation Committee and the Board of Directors. To strengthen the alignment between director compensation and sustainability performance, the Company has established the ESG and Information Security Committee, which regularly incorporates sustainability issues into the Board’s meeting agendas and decision-making processes. For directors who concurrently serve as the President and CEO, sustainability-related performance indicators have been included as key performance metrics. Additionally, the Company’s annual Board performance evaluations incorporate “sustainable strategy implementation and sustainability performance” as one of the assessment criteria, reinforcing director involvement in the Company’s sustainable development efforts and serving as a reference for determining remuneration.

The compensation package for senior executives/managers includes salary, retirement and pension benefits, holiday bonuses, and employee compensation (in the form of cash or stock). Among these, bonuses, compensation (cash/stock), and stock options are variable components and represent the primary portion of executive remuneration. Senior executives are also entitled to legally mandated insurance and retirement plans. The compensation of senior executives/managers is based on individual performance and is reviewed and assessed by the Compensation Committee. Recommendations are submitted to the Board of Directors for approval prior to execution.





Linking Incentive Systems and Sustainable Performance

Wistron aims to motivate senior executives, key professionals, and all employees to prioritize long-term, comprehensive performance and achieve sustainable operations. Since 2022, the Company has progressively linked the objectives of the six sustainability strategies and sustainability issues to the short- and long-term incentive compensation of the President and CEO, senior executives, and business unit heads. Sustainability performance indicators have been established to ensure that ESG efforts are integrated into overall company performance. For the President and CEO, sustainability-related indicators include the development of green products in response to climate change, the use of recycled materials, and expansion into the battery recycling industry. They also include increasing the use of renewable energy and improving energy efficiency at operational sites to reduce carbon emissions in alignment with the Science Based Targets initiative (SBTi) and achieving the 1.5°C reduction target. In a sustainable supply base, emphasis is placed on enhancing suppliers’ carbon reduction capabilities. On the social front, indicators include reducing occupational injuries and improving employee engagement. The relevant sustainability performance indicators are assigned to the responsible executive officer for each of the Six Sustainability Strategies, as well as to the corresponding business unit heads, who are tasked with developing and implementing the indicators.

Sustainability Performance Indicators			President & CEO	Business Unit Managers (Including main BG head)	Executive Officers (including heads of the Six Sustainability Strategy working groups)
Governance	Sustainable supply chain	Enhance the greenhouse gas inventory and energy management capabilities of high-energy-consuming suppliers	3%	15%	6%
	Green Products/ Product R&D and Innovation	Drive revenue through product innovation and increase the proportion of recycled or renewable materials in products	4%	15-25%	30%
Environmental	Circular Economy	Increase the use of recycled plastics and commercialize battery recycling solutions	1%	10%	10%
	Climate Strategy and Energy Management	Electricity Intensity	-	10%	15%
		Increase in the use of renewable energy and energy efficiency	10%*		
	Water Resource Management	Water usage intensity	-		
	Waste	Waste generation intensity	-	10-15%	10%
Social	Talent Attraction and Retention	Increase employee engagement and reduce turnover rate	1%		
	Occupational Health and Safety	Reduce occupational injuries and increase employee satisfaction	2%		
	Customer Relations	Customer satisfaction rate	-		-

Note: *Composed of 4% from President & CEO and 6% from Chief Sustainability Officer
 Presented on a weighted basis



5.2.2 Ethical Management

Policies and Organization

To establish a unified set of values and culture across all personnel, Wistron has adopted a [Code of Conduct](#), approved by the Board of Directors, as the highest standard of behavior for all employees of the Company, its subsidiaries, and joint ventures in which the Company holds significant impact. This Code serves as a guiding framework for all business activities. The Sustainability Office holds primary authority and responsibility for implementing this code, as well as establishing necessary procedures to ensure compliance.

To uphold ethical business practices, Wistron has established the [Code of Ethical Conduct](#), the [Ethical Corporate Management Best Practice Principles](#), and the [Corporate Governance Best Practice Principles](#). These policies require all employees to fully understand and comply with professional ethical standards, respect and strictly adhere to confidentiality agreements with clients, and refrain from accepting gifts or special treatment without proper cause. Wistron also engages customers, suppliers, business partners, and other stakeholders to promote a shared understanding of and commitment to the Company’s core values of integrity. The implementation status of integrity management is reported and reviewed annually by the Global Human Resources and Administration Division to the Board of Directors, the highest management body, at the end of each year.

Anti-Corruption Risk Management and Due Diligence

To ensure transparency and effectiveness in anti-corruption risk control mechanisms, Wistron regularly engages independent third-party organizations to audit and verify its compliance management system, thereby continuously reinforcing a strong culture of compliance.

Internally, the Company identifies Treasury Management & Corporate Communications, Global Supply Chain Management, and Administration Services as potential high-risk areas. These departments are subject to internal audit or periodic job rotations. Additionally, managerial staff in these functions are required to attend external training programs offered by professional institutions to enhance their understanding of legal compliance.

Externally, before establishing business relationships with agents, suppliers, customers, or other partners, the Company assesses the legality of their business practices, the presence of integrity-related policies, and any history of unethical conduct. During the course of business, Wistron communicates its integrity management policy and related internal regulations in accordance with internal procedures. Contract terms include requirements to comply

with Wistron's anti-corruption policies, which cover reasonable and transparent payment terms, the handling of misconduct and violations related to commissions, kickbacks, or other improper benefits. Wistron maintains a firm stance against offering, promising, requesting, or accepting any form of improper advantage, whether directly or indirectly. If unethical behavior is identified, business dealings are immediately terminated, and the entity is blacklisted. During the period from 2021 to 2024, no corruption or bribery was found in the reported cases after investigation, and no penalties were imposed by the competent authorities for related cases.

Commitment and Support

To ensure that all personnel fully understand relevant regulations and expectations, Wistron continuously implements education, training, and awareness programs. For members of the Board of Directors, all have completed the signing of the Code of Conduct Acknowledgment Form, and dedicated training sessions on the prevention of insider trading have been arranged to reinforce their corporate governance responsibilities in upholding integrity. For all new employees, the Company requires reading and signing the [Code of Conduct](#) Acknowledgment Form and completing an online ethics training course. In 2024, both the acknowledgment and training completion rates reached 100%. For existing employees, annual training on the Code of Conduct, including anti-corruption and anti-bribery topics, is mandatory for all personnel across all facilities. In 2024, the training completion rate for all employees was also 100%, reflecting Wistron’s strong commitment to fostering a culture of integrity.

Code of Conduct Training and Acknowledgment

Item	2021	2022	2023	2024
Code of Conduct Coverage Rate (%)	100%	100%	100%	100%
Code of Conduct Signing Rate (%)	99.9%	100%	100%	100%
New Employee Training Coverage Rate (%)	100%	100%	100%	100%
Regular Training Coverage Rate for All Employees (%)	100%	100%	100%	100%
Training Completion Rate for All Employees (%)	99.9%	100%	100%	100%



Type	Code of Conduct Training Rate	Taiwan	Overseas
Years of Service	New Employees	2,936 (100%)	6,150 (100%)
	Current Employees	10,562 (100%)	22,593 (100%)
Employment Type	Direct employees	4,260 (100%)	19,552 (100%)
	Indirect employees	9,238 (100%)	9,191 (100%)
Location	Administrative	7,110 (100%)	29 (100%)
	Manufacturing	6,388 (100%)	28,714 (100%)

Whistleblowing and Disciplinary Measures

For any inquiries regarding the Code of Conduct, both internal and external stakeholders can contact the Sustainability Office. Subsidiaries and joint ventures where Wistron have a significant impact have established their own consultation channels to engage with stakeholders.

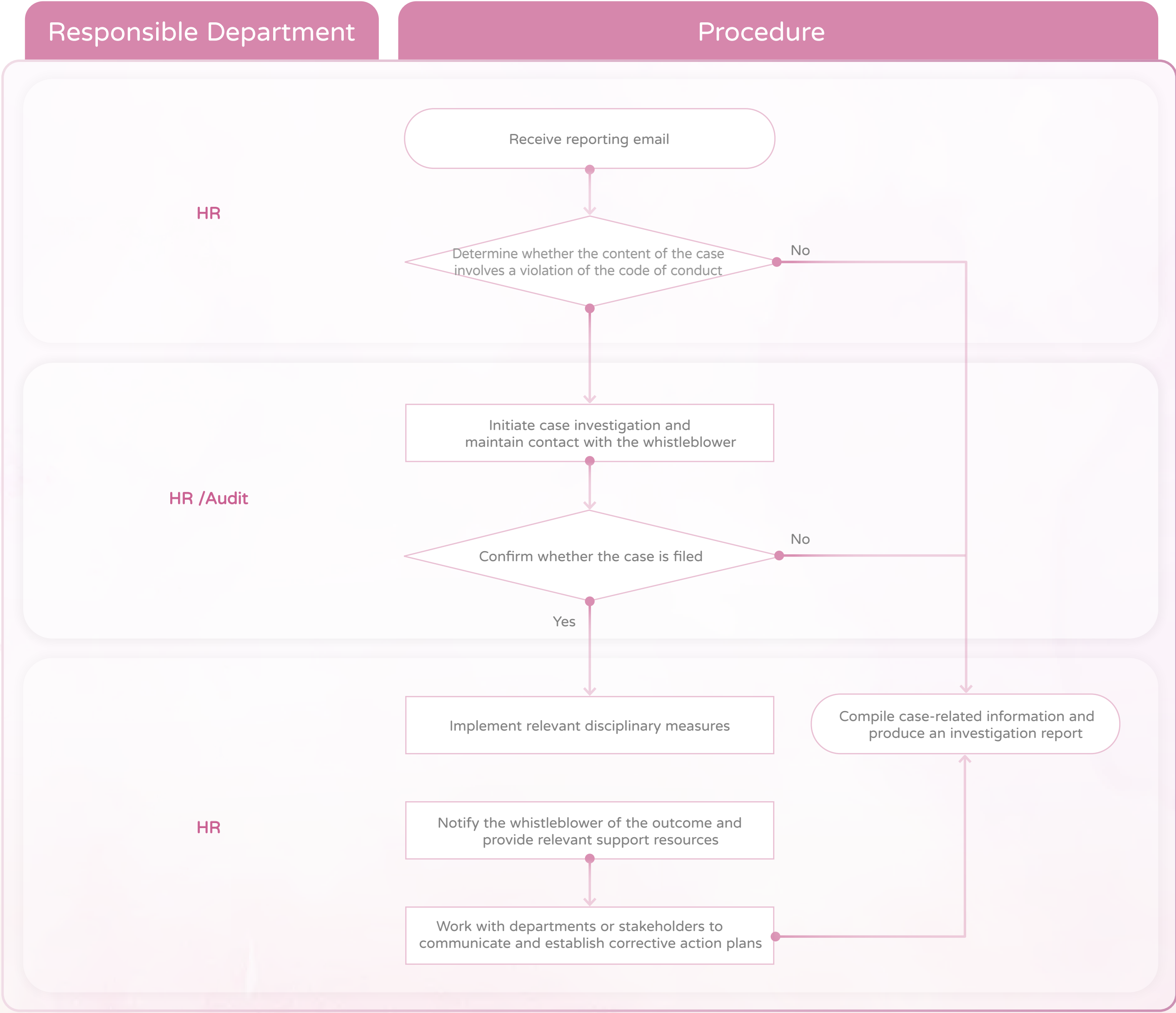
Wistron encourages all employees and external stakeholders to report unethical conduct or violations of business ethics through its whistleblowing channels. The Company is committed to maintaining the confidentiality of whistleblower identities and report contents, and accepts anonymous submissions to ensure whistleblowers are protected from any form of retaliation or unfair treatment. The Company enforces a zero-tolerance policy toward any violations of the Code, including retaliation against whistleblowers, and will take disciplinary action in accordance with the Code of Conduct.

To ensure employees are familiar with the whistleblowing channels and related mechanisms, Wistron includes relevant information in onboarding and Code of Conduct training. The Company also promotes awareness through public information boards and the internal website, educating employees on when and how to report, available reporting channels, processing procedures, and whistleblower rights. This helps foster a proactive culture of integrity

and strengthens the Company's whistleblowing system.

A dedicated email address (ethic@wistron.com) is available for reporting violations of the Code of Conduct. These cases are primarily handled by the Global Human Resources and Administration Division, with investigation and handling procedures outlined in the following diagram. An annual report on case handling is submitted to the Board of Directors, and the Audit division is responsible for overseeing the investigation and resolution process.







Code of Conduct Reports / Filed Cases		2021	2022	2023	2024	
					Number of Cases	Number of Filed Cases
Business Ethics and Operations	Corruption and Bribery	0	0	0	4 ¹	0
	Conflicts of Interest	0	0	0	1 ²	0
	Fair Competition	0	0	0	2 ³	0
	Money Laundering or Insider Trading	0	0	0	0	0
	Trade Secrets	0	0	1	5 ⁴	1
	Privacy / Personal Data Protection	0	0	0	0	0
	Other (Political Contributions, Charitable Donations, and Social Engagement)	0	0	0	0	0
	Total Number of Business Ethics and Operational-Related Cases	0	0	1	12	1
Protection of Human Rights	Discrimination	0	0	0	3 ⁵	0
	Harassment	0	3	1	3 ⁶	0
	Occupational Safety and Health	0	0	1	1 ⁷	0
	Total Number of Human Rights-Related Cases	0	3	2	7	0
Environmental Protection	Total Number of Environmental Protection-Related Cases	0	0	0	0	0
Total		0	3	3	19	1

- Note:
- Two reports alleged that procurement personnel in the Taiwan office had accepted bribes, one report alleged bribery involving a supplier at the Malaysia plant, and another reported bribery by a member of the headquarters construction department. Investigations found no conclusive evidence in any of these cases.
 - One report claimed that Wistron assets were being sold externally; however, an investigation confirmed that the items were not Company-owned assets.
 - One report alleged a subsidiary failed to fulfill a procurement contract. After negotiation, both parties reached an agreement on the terms. Another report raised concerns about flaws in the contract process for copiers at the Hsinchu plant; however, the investigation found that no new contracts were being discussed at that time.
 - One report warned of external poaching activities; relevant department heads were advised to stay alert and take preventive measures. Another report alleged the misuse of a corporate employee account by Wistron personnel; however, the investigation confirmed that the individual was not affiliated with Wistron. One report alleged that external individuals had entered a lab in the Taiwan office; no conclusive evidence was found. Another report claimed the Kunshan plant had used unauthorized fonts for event materials; this was found to be part of a phishing scheme. One report confirmed unauthorized font use in the Taiwan office. Legal representatives completed a licensing agreement with the font owner. Internally, the Company mandated the use of open-source fonts for promotional activities and software development projects. Special font usage now requires prior evaluation and contract approval by the responsible management unit.
 - One Malaysia plant employee reported unfair bonus distribution; the issue was resolved through communication and mutual agreement. One report alleged discrimination by current management at the former India plant. As Wistron no longer has jurisdiction, the complainant was advised to contact the local company representative. One Czech plant employee reported that their contract was not renewed due to religious discrimination; however, an investigation found that the non-renewal was performance-related.
 - One report involved a romance scam allegedly committed by a Taiwan office employee; the investigation confirmed the individual was not a Wistron employee. One report alleged harassment by a former employee of the Taiwan office; the person in question had already left the Company. Another report claimed verbal bullying by a supervisor in the Taiwan office; investigation found the allegations to be unsubstantiated.
 - One anonymous report alleged that production line staff at the Hsinchu plant were not following occupational safety and health regulations. As further details could not be obtained, the relevant department was reminded of safety protocols and received additional training.



Key Issues in Integrity Management

Anti-Competitive Practices

Integrity in business is a fundamental corporate social responsibility. Wistron has established the [Ethical Corporate Management Best Practice Principles](#), requiring all employees to conduct business activities in accordance with fair competition laws. Employees are prohibited from engaging in price-fixing, bid rigging, production or quota restrictions, or market sharing and allocation practices based on customers, suppliers, geographic areas, or types of business. Wistron strictly complies with all applicable laws and regulations across all aspects of business operations. From 2021 to 2024, the Company did not incur any penalties from authorities for violations related to anti-competitive behavior or monopolistic practices.

Political and Charitable Contributions

Wistron adheres to a policy of political neutrality and does not actively participate in political parties or political activities, nor does it engage in lobbying. Should any political contributions be considered, the Company will strictly comply with all relevant laws and regulations, ensuring that such contributions are not used to gain business advantages or influence transactions. Wistron firmly avoids the misuse of political or charitable donations as a means of corruption and bribery. From 2021 to 2024, the Company did not make any political contributions. However, Wistron respects employees’ freedom of political expression and encourages them to fulfill their civic responsibilities. In terms of public welfare and charitable giving, all donations and sponsorships are governed by internal management regulations, which strictly prohibit disguised bribery or personal gain. These rules ensure compliance with anti-corruption standards and legal requirements.

Supplier Integrity Management

Wistron has established a [Supplier Code of Conduct](#) that clearly outlines the behavioral standards and expectations for its supply chain partners. In addition to communicating Wistron's anti-corruption policies through training courses on the Wistron Global Learning Platform, the Company reinforces its integrity management principles and policies each year at the annual supplier conference, where it also shares information on dedicated whistleblowing email channels. As a result of these ongoing awareness efforts and management mechanisms, there were no reported incidents of corruption or ethical misconduct by Wistron suppliers in 2024.

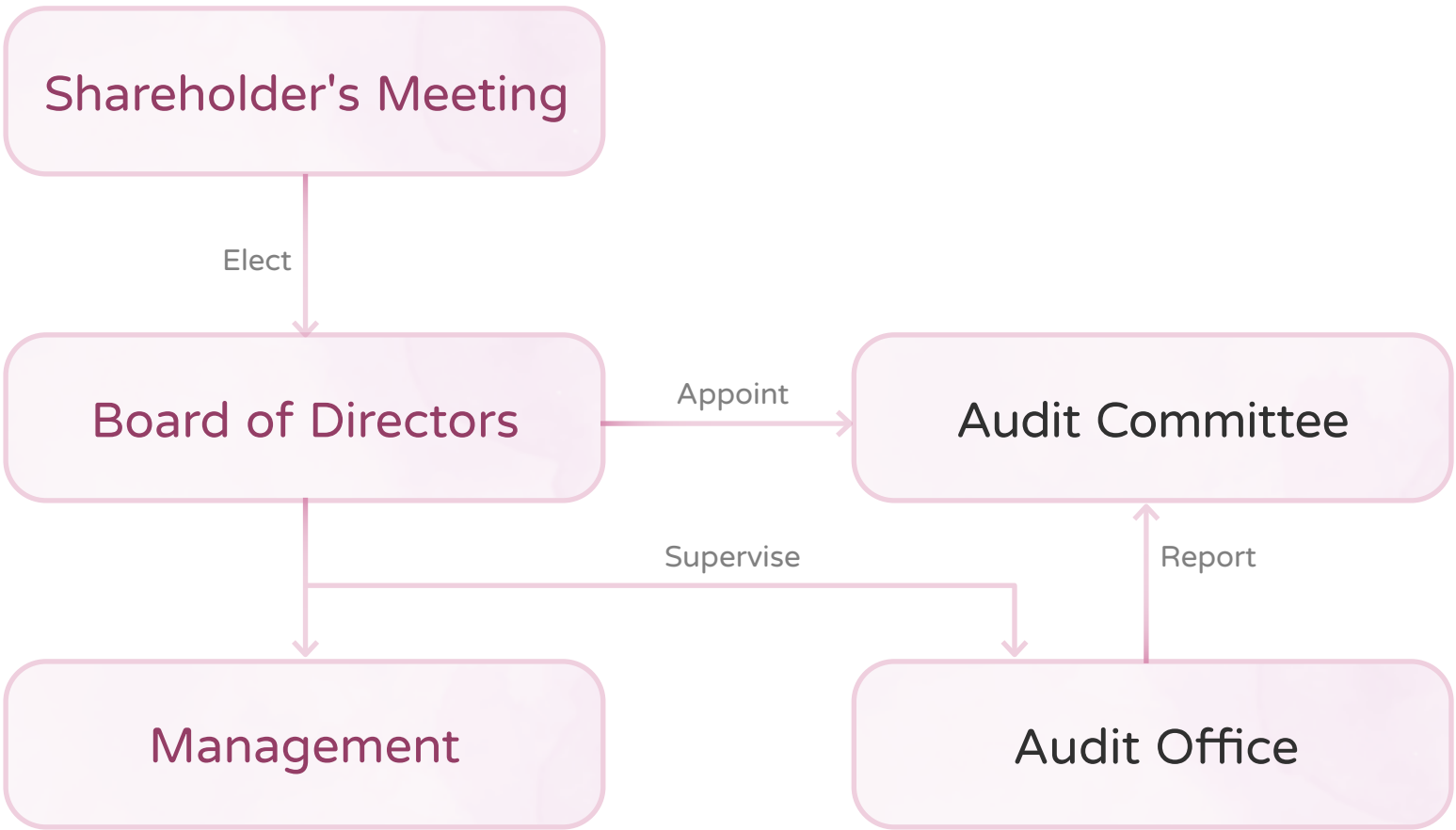
The Company has set up a dedicated whistleblowing and grievance email account for suppliers (GSCM_Office@wistron.com). Reports of violations of the Supplier Code of Conduct are handled by the Global Supply Chain Management team. In 2024, there were no reported cases, and no contract terminations occurred due to breaches of integrity.

Internal Control and Internal Audit

Internal Audit

Wistron Corporation has established an Audit Committee, composed entirely of independent directors, under the Board of Directors. An independent Internal Audit Department, which reports directly to the Board of Directors and the Audit Committee, is in place. In addition to regularly reporting audit activities to the Audit Committee, the Head of Internal Audit is also required to attend Board meetings to deliver reports and may report to the Chairperson and the Audit Committee at any time when necessary.

Internal Audit Organization



Note: The Internal Audit Office is staffed with qualified and competent audit professionals



Audit Objectives

Wistron Corporation's internal audit philosophy prioritizes value creation over fraud prevention. Experienced and competent personnel are selected to perform audit duties. Through risk assessments, system reviews, and on-site inspections, the Internal Audit Department assists various departments in identifying areas for process improvement and encourages self-driven enhancements. These efforts aim to improve overall operational performance and create greater value for shareholders and stakeholders.

Audit Operations

At the end of each year, the Internal Audit Department conducts a risk assessment based on changes in the operating environment, regional characteristics of subsidiaries, future business strategies, and findings from previous audits. Based on this assessment, the department formulates key audit areas and prepares the annual audit plan, which is submitted to the Audit Committee for review and then approved by the Board of Directors for implementation.

Audit results are reported in writing to the Audit Committee by the end of the following month. Any concerns are further addressed via email or phone communication. On a quarterly basis, key audit findings are reported to senior management and presented to the Board of Directors. If circumstances change during the execution of the audit plan, adjustments are made as needed, subject to approval by the Board of Directors.

Each quarter, the Board of Directors and Audit Committee invite a Certified Public Accountant to present findings and recommendations from the financial report review or audit. The CPAs engage in two-way communication with the independent directors, the Chief Financial Officer, and the Head of Internal Audit. Other relevant managers may also be invited to attend as necessary.

Self-Assessment of Internal Controls

Wistron's internal control system is designed by management in accordance with the "Regulations Governing the Establishment of Internal Control Systems by Public Companies" and approved by the Board of Directors, taking into account the company's overall operations. The internal control system consists of key components and control activities intended to reasonably ensure the achievement of the following objectives:

- 1. Operational effectiveness and efficiency
- 2. Reliability, timeliness, transparency, and regulatory compliance of reporting
- 3. Compliance with applicable laws and regulations

The internal control system adopts a digital platform for self-assessment operations. The President & CEO supervises and encourages all internal departments and subsidiaries to conduct self-assessments on their internal controls at least once per year. The Internal Audit Department reviews these self-assessment reports, together with the status of improvements to any deficiencies or irregularities previously identified through audit activities. This comprehensive review forms the primary basis for the Chairman and the President & CEO to assess the overall effectiveness of the internal control system and to issue the Internal Control System Statement.

The Internal Audit Department conducts evaluations in accordance with the "Internal Auditing Implementation Rules" to assess the adequacy of the internal control system and the effectiveness of its implementation in day-to-day operations. Both ongoing and project-based audits are conducted, encompassing all internal operations and subsidiaries of the Company. Based on the results of risk assessments, the Internal Audit Department develops an annual audit plan, which is reviewed and approved by the Board of Directors and subsequently implemented. Monthly audit reports are submitted to the Audit Committee for review,

and any identified deficiencies are subject to ongoing follow-up until rectified.

Through effective implementation of internal control practices, Wistron did not identify any material internal control deficiencies in 2024. On a quarterly basis, the Head of Internal Audit attends both Audit Committee and Board meetings to report audit findings.

Audit Management of Subsidiaries

In consideration of local legal requirements and the operational nature of each subsidiary, Wistron supervises and guides subsidiaries to establish appropriate control measures for oversight and management as needed. All subsidiaries are included within the scope of internal audits. Audit activities are carried out based on risk assessment results. For any internal control deficiencies or irregularities identified by the Internal Audit Department, thorough communication is conducted with the audited units, which are required to propose specific and effective corrective measures. The Internal Audit Department continues to follow up on these issues until full resolution is achieved.





5.2.3 Legal Compliance

Wistron has established a comprehensive set of internal operational procedures in accordance with relevant regulations governing public companies. The Company continuously monitors regulatory updates from competent authorities and promptly adjusts internal policies as needed, requiring all subsidiaries within the Group to comply and ensure lawful operations.

In addition, the management team closely monitors domestic and international policies and regulations that may affect the Company’s financials and business operations. In response, the Company not only adjusts its risk management procedures accordingly but also promptly updates related training programs to reflect the latest regulatory requirements. The Training Center is responsible for coordinating these programs and engaging internal and external professional instructors. Training initiatives include, but are not limited to, onboarding programs, compliance training for managers and legal personnel, and company-wide compliance education. Post-training evaluations, such as exams or surveys, are conducted to ensure learning effectiveness. Through continuous education and training, the Company strengthens employees’ legal awareness and professional capabilities, ensuring that all personnel adhere to current regulations in their interactions with customers.

From 2021 to 2024, the Company did not incur any significant fines (exceeding NT\$1 million) for violations of laws or regulations, including but not limited to product safety, marketing, communications, or business ethics. However, during 2023 and 2024, a total of six minor monetary penalties related to labor, occupational safety and health, and environmental regulations were recorded, amounting to NT\$195,500 in fines and 4 hours of mandated environmental training. Relevant internal management mechanisms have since been strengthened to prevent recurrence.



5.3 Risk Management

Wistron adheres to a philosophy of sustainable operations. Through the establishment, implementation, and maintenance of proactive risk management mechanisms, the company continuously monitors internal and external issues and environmental changes. It conducts operational impact analyses and develops effective and flexible responses to address challenges. Regular self-assessment and ongoing improvements enhance the company's resilience, fulfilling its commitment to uninterrupted operations and safeguarding the best interests of customers and stakeholders. Additionally, Wistron effectively manages operational risks and fosters a risk-aware culture through continuous optimization of education and training, performance management, risk assessment, early warning notifications, and public disclosures.

5.3.1 Enterprise Risk Management

Risk Governance Structure

Wistron adheres to the principles outlined in ISO 31000 – Risk Management Guidelines and adopts the “Three Lines of Defense” framework to systematically assess and manage potential risks that could impact business operations. With active involvement from the Board of Directors, the Company ensures comprehensive risk governance. In 2023, the Board of Directors approved the [Risk Management Policy and Procedures](#), which formally integrates risk management into operational activities and daily management processes to achieve the Company's risk management objectives.

Board Oversight Responsibilities

The Board of Directors is the highest supervisory body for risk management at Wistron. It is responsible for approving risk management policies and related guidelines, ensuring effective implementation of the risk management framework. To fulfill its supervisory duties, the Board authorizes the Audit Committee to assist in overseeing the risk management mechanisms and their implementation. The Audit Committee reviews the effectiveness of risk management operations annually, provides recommendations for improvement, and reports to the Board to ensure strategic goals are met and stakeholder interests are protected.



Three Lines of Defense Framework

Wistron adopts the Three Lines of Defense model to establish a multi-level, structured risk control mechanism that enhances internal controls and corporate governance. Responsibilities are clearly defined and coordinated across the organization to improve overall risk management effectiveness:

First Line of Defense:
Business and Operational Units



Business and production units serve as the primary entities responsible for executing daily risk management activities. Designated personnel from each business unit—appointed by members of the Risk Management Team—carry out risk management practices. Together with relevant staff, they conduct enterprise-level and operational-level risk identification at least once a year. These teams analyze and assess various risk scenarios, develop response strategies, and implement routine risk control procedures.

Second Line of Defense:
Risk Management and Compliance



The Risk Management Team, reporting to the Audit Committee, leads this line of defense. It collaborates with the finance, accounting, and legal departments to ensure compliance and promote a strong risk management culture. The Risk Management Team, composed of the heads of all business units and chaired by the Chief Financial Officer, meets monthly to review risk developments. It reports its findings to the Audit Committee and the Board of Directors semiannually and prepares an annual Risk Management Report. The chairperson designates team members to serve in the Risk Management Office, which is responsible for executing day-to-day risk management tasks and coordinating activities across departments.

Third Line of Defense:
Internal Control and Audit



The Internal Audit Department and the Audit Committee make up the third line of defense. They oversee company operations and provide a systematic approach to strengthening risk management and internal control execution. The Audit Department, which reports directly to the Board, conducts independent audits in accordance with the Risk Management Policy and Procedures to evaluate the effectiveness of risk management activities and recommend improvements. Audit results are reported to the Board annually to ensure risk strategies are implemented and risks are properly controlled.



Risk Management Procedures

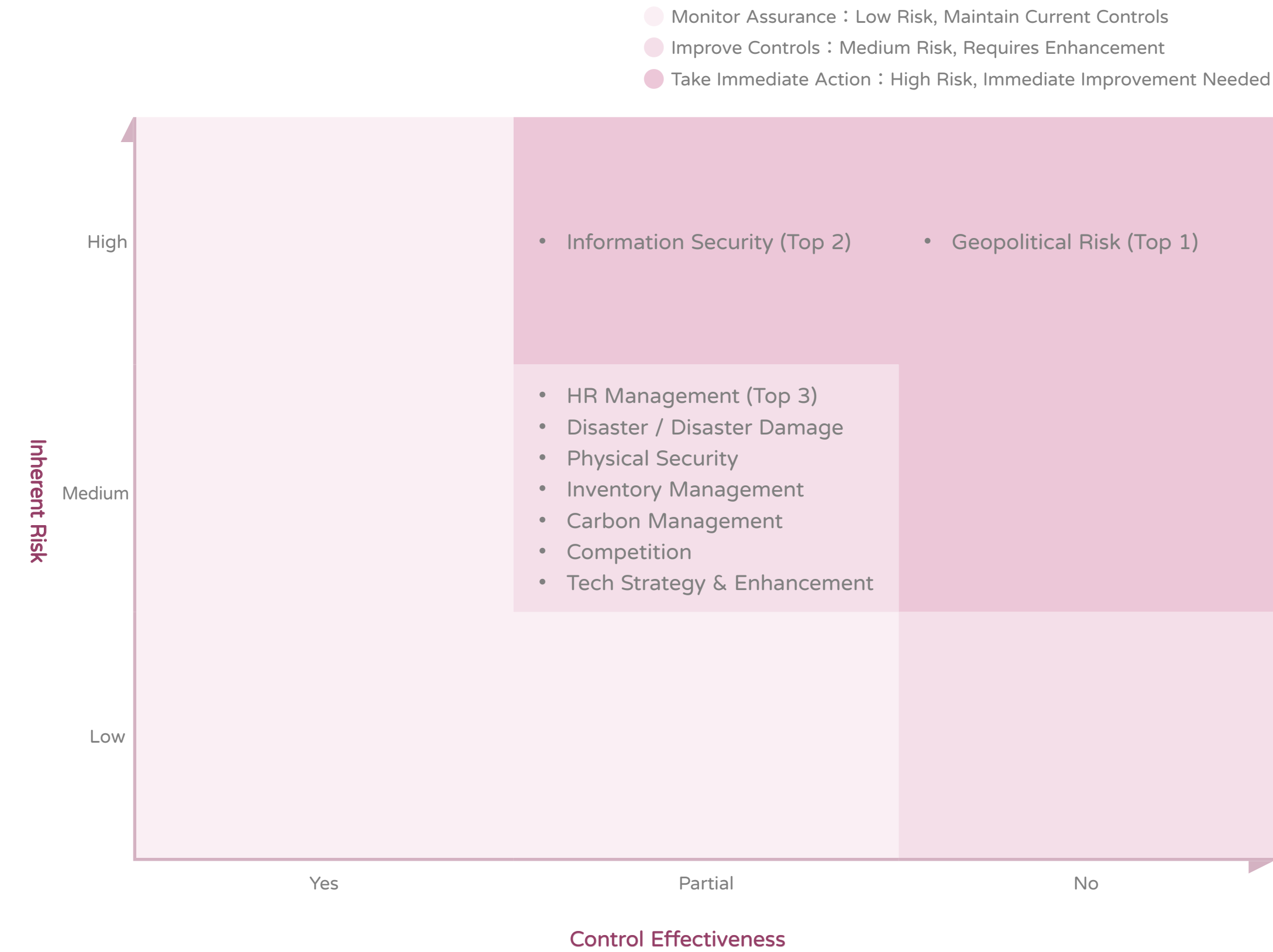
Wistron has established a comprehensive risk management process encompassing the following stages: risk identification, risk analysis, risk evaluation, risk response and monitoring, and risk reporting and disclosure. This systematic approach enables the Company to effectively identify, assess, and respond to various types of risks, ensuring business continuity and optimal allocation of resources. Each year, the Risk Management Team requests the respective risk management working groups to evaluate and discuss potential and emerging risks based on indicators such as likelihood of occurrence, severity of impact, and effectiveness of existing controls. The results are regularly reported to the Audit Committee and the Board of Directors.





Risk Identification

In 2024, the Risk Management Team conducted a risk assessment using structured questionnaires, taking into account the likelihood of occurrence, severity of impact, and effectiveness of existing controls. A total of nine key medium-to-high-level risks were identified. Among these, two annual risks were assessed with a residual risk level of T – Take Immediate Action (requiring immediate remediation), and seven were rated as I – Improve Controls (requiring improvements to controls or response measures).



Risk Sensitivity Analysis and Stress Testing

To strengthen the Company’s risk awareness, the Risk Management Team regularly conducts sensitivity analysis and stress testing on significant risks that may impact operations. Risk sensitivity analysis quantifies the potential financial impact of different risk scenarios. Stress testing simulates severe risk fluctuations to help the Company understand its tolerance under extreme conditions. These analyses and tests support more accurate risk assessment, management, and response, ensuring operational stability and long-term sustainability.

Types of risk	Scenario Analysis	Results of Sensitivity Analysis and Stress Testing
Foreign Exchange Risk	The Company's exchange rate risk primarily arises from foreign-currency-denominated cash, accounts receivable, borrowings, accounts payable, and other assets, which may result in foreign exchange gains or losses upon conversion. The major foreign currency exposures are in USD and CNY.	Based on the position calculation as of 2024.12.31, if the New Taiwan Dollar appreciates or depreciates by 405% against the U.S. dollar and Chinese yuan, the Company’s net income after tax for 2024 would be affected by approximately NT\$1 billion, reaching a level classified by the Company as having a material impact.
Interest Rate Risk	Interest rate risk is assessed based on the Company’s total outstanding liabilities and their remaining maturity.	Based on total liabilities as of 2024.12.31, a change in interest rates of ±300 basis points would affect the Company’s 2024 net income after tax by approximately NT\$1 billion, which also constitutes a material impact as defined by the Company.
Geopolitical Risk	In the event of escalating geopolitical tensions affecting production sites in Taiwan and Mainland China, the Company estimates potential business interruption losses by simulating factory shutdown durations.	If a production halt extends to 20 days, the resulting business interruption loss would exceed NT\$1 billion, reaching the material impact threshold as defined by the Company.



Risk Appetite

The Risk Management Team defines the Company’s annual risk appetite based on strategic objectives and the balance between risk and return. Once approved by the Audit Committee and the Board of Directors, the defined risk appetite is communicated and implemented across all business units. Risk appetite is categorized into five levels, each corresponding to a defined range of potential financial loss. These levels are linked to specific preventive and mitigation measures, ensuring that all critical risks are effectively managed.

Level	Impact Classification	Estimated Financial Loss (NT\$)
1	Extremely Minor	<= 1 million
2	Minor	1 - 10 million
3	Medium	10 - 100 million
4	Severe	100 million – 1 billion
5	Extremely Severe	>= 1 billion





Risk Prioritization, Response, and Monitoring

Senior management and the Risk Management Team convene semiannual risk meetings to review the implementation results of risk management activities. Following discussion and risk prioritization, the top three material risks identified for the Company in 2024 are: Geopolitical Risk, Information Security/Cybersecurity Management Risk, Human Resources Management Risk. The responsible units for each risk are required to develop corresponding risk response action plans. These plans are reviewed and confirmed by the respective unit heads, and subsequently submitted to the Audit Committee and the Board of Directors for regular evaluation and review.

Types of risk	Description of Risk	Mitigation Measures	Assessment Methods
Geopolitical Risk	Rising tensions between the two sides of the Taiwan Strait have heightened the risk of potential armed conflict in the region	<ol style="list-style-type: none">1. Regularly review geopolitical issues relevant to the company's operations or those of its business partners' locations2. Develop a comprehensive command structure and operational headquarters relocation plan, covering order fulfillment, material procurement, manufacturing, IT systems, cash flow, logistics, and personnel transition & reach consensus with key clients regarding relocation3. Regularly evaluate the impact of internal and external environmental factors, and adjust production capacity accordingly to ensure optimal allocation based on customer demand. This approach reduces reliance on any single region, mitigates geographic risks, and enhances production flexibility.4. Promote production automation to enhance manufacturing efficiency and adaptability to changing environments, thereby mitigating the operational impact of geopolitical risks.	<p>An armed conflict in the Taiwan Strait could lead to large-scale political, economic, and social upheaval across both sides of the Strait, with far-reaching implications for regional stability. Such a conflict may disrupt supply chains, trigger large-scale capital outflows, and sharply reduce cross-border trade, potentially affecting the economies of neighboring countries as well as global markets. Given Taiwan Strait's critical strategic importance, any escalation could severely impact the global electronics supply chain and shipping logistics, leading to production halts in key industries and heightened uncertainty.</p> <p>For Wistron, the outbreak of such a conflict could result in operational disruptions exceeding seven days, property losses surpassing NT\$1 billion, and casualties of more than three employees. More broadly, it may trigger a crisis of market confidence, undermining the Company's long-term competitiveness and brand image. Although Wistron has accelerated the establishment of overseas production sites to mitigate geopolitical risks, it remains essential to continuously strengthen risk management frameworks. This includes developing robust contingency plans, deepening partnerships with overseas clients, and enhancing the Company's overall resilience to the operational impacts of potential conflicts.</p>
Operational disruptions caused by cybersecurity risks	Lack of a Zero Trust Architecture makes it difficult to assess Wistron's level of cybersecurity maturity under this model; Lack of clear AI governance framework, structure, management processes, and protection mechanisms	<ol style="list-style-type: none">1. Enhance Zero Trust cybersecurity defenses by implementing multiple initiatives based on scope and criticality2. Enhance AI governance mechanisms by implementing a range of AI governance initiatives based on scope and criticality	<p>In recent years, the rapid advancement of generative AI technology has significantly empowered malicious actors, accelerating the evolution of social engineering attacks and expanding the scope of cyberattacks. Generative AI enables hackers to overcome language barriers when crafting malicious emails and messages, substantially reducing grammatical and lexical errors and thereby making such communications appear more authentic. Furthermore, attackers can leverage generative AI to automate the collection of target-specific information, facilitating more personalized and sophisticated whaling attacks aimed at corporate executives.</p> <p>With the rise of new threats, security awareness training alone is no longer enough to protect against risks. Should such a scenario occur, the resulting ransom demands could exceed NT\$1 billion, and the incident may attract adverse media coverage both domestically and internationally, leading to significant reputational damage.</p>
Human Resources Management	Amid shifting global and regional economic conditions, the demand for talent in Taiwan's technology industry continues to grow, intensifying competition—particularly in the recruitment of international talent. Future challenges in this area are expected to become increasingly complex.	<ol style="list-style-type: none">1. Enhance internal and external networking efforts by actively participating in industry and academic events, seminars, and communities to build strong networks for both local and international talent.2. Reassess recruitment needs by expanding outreach to a broader range of educational institutions and exploring new recruitment channels, including industry-academia cooperative graduate programs.3. Continue to strengthen employer branding by building an attractive and competitive brand image—highlighting company culture, benefits, and growth opportunities—and integrating themes such as AI and digital innovation to attract and retain top technology and international talent.4. Provide professional development and growth opportunities through internal training programs, academic collaborations, and participation in international conferences, enabling talent to grow and develop within the organization. Additionally, implement structured development plans for key internal talent to align with the Company's long-term strategic direction.	<p>By 2025, Taiwan will officially become a super-aged society, with over 20% of its population aged 65 and above. The National Development Council projects that following a peak of 23.6 million in 2019, Taiwan's total population will shrink to 16.22 million by 2070. This indicates that Taiwan will face significant challenges related to population decline and aging in the coming decades.</p> <p>As experienced employees gradually retire, businesses are confronted with the dual risks of talent loss and skill gaps—particularly in fields that require high levels of expertise and technical knowledge. The scale of the incoming workforce is insufficient to fully offset the operational demand for experience and specialized capabilities. While the short-term impact on the Company remains limited, in the long run, failure to recruit and develop sufficient high-caliber talent may erode the Company's current industry leadership, with potentially significant consequences for market share and overall competitiveness.</p>



Emerging Risk Management

Since 2020, Wistron has annually referenced the latest external risk insights—such as the World Economic Forum’s Global Risks Report—to systematically identify emerging risks through four key procedures: understanding the industry context, conducting risk assessments (including identification, analysis, and evaluation), implementing risk treatment, and performing ongoing monitoring and review. By broadly gathering professional insights from management, Wistron proactively identifies potential emerging risks, formulates appropriate mitigation measures, and reports to the Audit Committee and the Board of Directors on a regular basis to ensure the Company can implement forward-looking response strategies.

Based on the Risk Management Team’s latest assessments conducted between the end of 2024 and early 2025, Wistron has identified generative AI risks, geopolitical risks, population aging and recruitment challenges, and emerging technology risks as key current emerging risk items. The Company will continue to closely monitor the development and potential impacts of these risks to ensure its risk control measures remain forward-looking and adaptive.



Internal and External Audits of Enterprise Risk Management

Wistron has established a comprehensive internal and external audit mechanism to ensure the effectiveness and compliance of its risk management systems. For internal audits, the Audit Department is responsible for developing the annual audit plan, conducting risk-based audits, and reviewing the compliance and effectiveness of risk management activities. Audit results and recommendations for improvement are reported regularly to the Board of Directors and the Audit Committee. In addition, Wistron periodically engages third-party institutions to assess the design and implementation effectiveness of its risk management systems. The results of these external audits are incorporated into improvement plans to ensure alignment with international standards and ongoing optimization. Findings from both internal and external audits are consolidated by the Risk Management Team. After being reviewed by senior management, they are reported to the Audit Committee and the Board of Directors on a regular basis, further enhancing the long-term effectiveness and resilience of the Company’s risk management systems.



Shaping A Risk Management Culture

Wistron places strong emphasis on fostering risk awareness across all levels of the organization. In addition to conducting company-wide training on risk-related topics, Wistron integrates risk management into daily operations by aligning it closely with performance evaluation indicators to embed risk culture into the corporate culture.

Incentive Mechanisms for Risk Management

Wistron has established differentiated performance evaluation standards for employees at various levels, incorporating key risk indicators, such as human capital management and information security/cybersecurity, into the scope of performance assessments to ensure the effective implementation of risk management.



Wistron closely integrates risk management with performance evaluation, with a particular focus on the management outcomes of specific risk areas such as human capital, to ensure effective control and continuous improvement of related risks. Annual objectives for senior managers include clear targets related to employee engagement and satisfaction, turnover rate, and workplace injury rate. These quantified performance metrics are designed to ensure the stability and effectiveness of human capital management. Moreover, the company regularly assesses results in these areas, and the achievement of related performance indicators serve as a key basis for determining compensation. This approach reinforces a positive feedback loop between Risk management performance and incentive outcomes.



Wistron incorporates information security and cybersecurity as a key risk area in its performance evaluation framework to ensure accountability and proactive management. For example, in the area of human capital, management indicators for mid-level and junior managers are cascaded from senior executives and allocated based on departmental responsibilities. These include specific metrics such as "employee engagement/satisfaction," "turnover rate," and "work injury rate," and are subject to regular performance evaluations. Through this top-down breakdown of indicators and performance monitoring, Wistron ensures that accountability for human capital management is effectively implemented at all organizational levels.



General employees

Wistron is committed to integrating information security/cybersecurity risk controls into its performance appraisal framework to ensure that risk awareness is fully embedded at every level of the organization. To reduce the impact of information security/cybersecurity risks on business operations, the Company conducts employee training programs and simulated social engineering exercises to strengthen awareness and alertness. Additionally, violations of information security/cybersecurity policies by departmental employees are factored into the performance appraisal indicators of department heads. Individual violations are directly reflected in each employee's performance appraisal rating, reinforcing accountability and promoting a culture of security awareness.

Risk Management Trainings

In accordance with Article 16 of the “Corporate Governance Policy”, Wistron shall provide directors risk management training programs every year. The course must contain the risk management principles for Wistron to continuously strengthen the Board's risk management capabilities.

Furthermore, Wistron integrates risk management into its training system, not only to enhance the risk awareness of all employees but also to strengthen the resilience and competitiveness of the entire organization. In 2025, we incorporated diverse teaching methods, covering all employees from entry-level staff to senior management of Wistron and its subsidiaries, with the goal of comprehensively improving employees' capabilities and practical skills in risk management. Through this large-scale and systematic training program, a total of 44,253 employees across our global operations completed the training, accumulating a total of 7,376 training hours.

Recognizing risk management as a crucial competency in today's dynamic global landscape, the training emphasizes practical application, fostering a proactive, company-wide risk management culture. We are committed to continuously enhancing the curriculum with relevant emerging risk topics to ensure our workforce maintains a forward-looking perspective and strong risk awareness, supporting Wistron's sustainable growth.

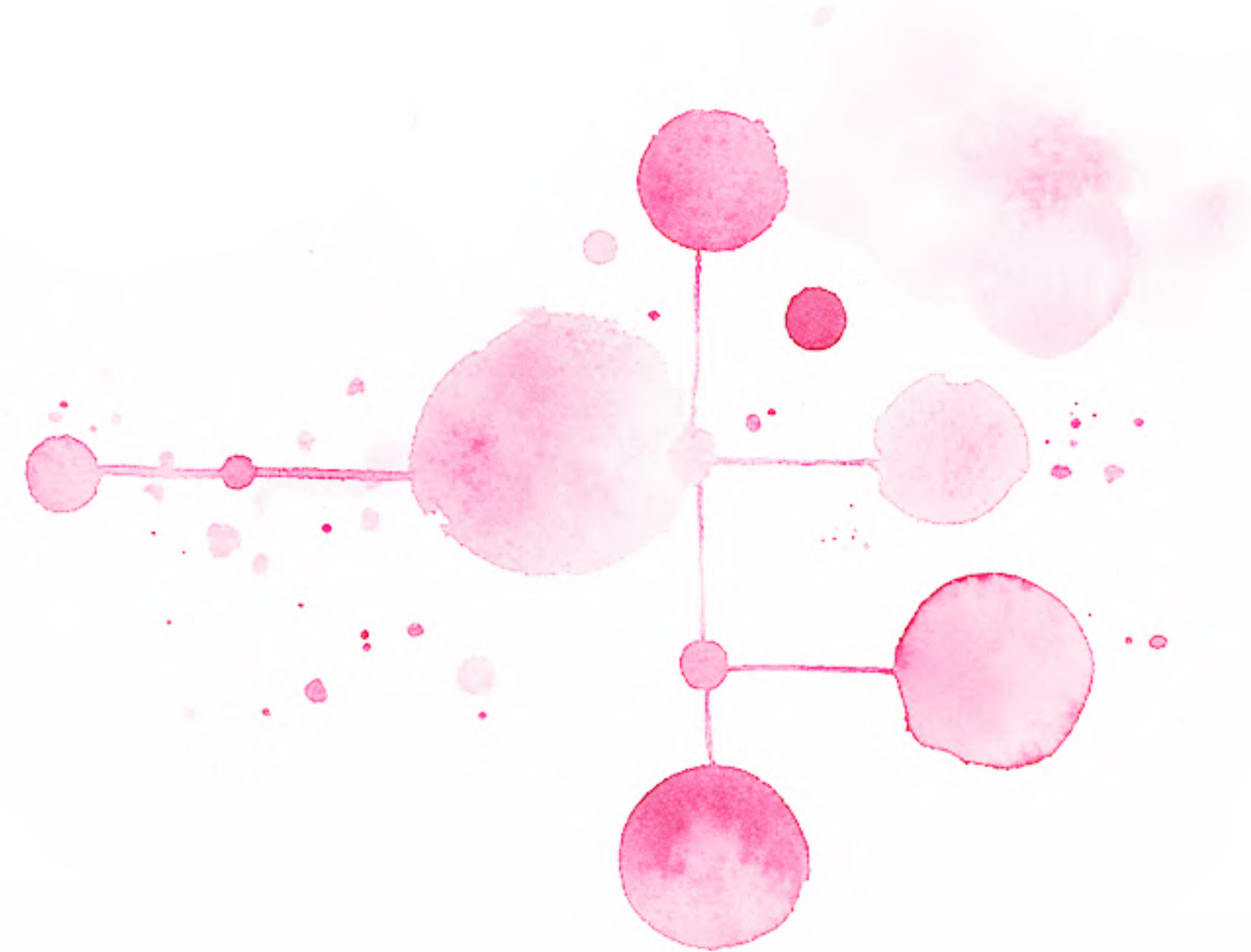


Integrating Risk Criteria into Product and Service Development

Wistron incorporates risk criteria across all stages of product and service development to systematically assess the severity of potential impacts, ensuring quality and regulatory compliance. During the development phase, Failure Mode and Effects Analysis (FMEA) and a "lessons learned" database are used to assess potential risks. In the design phase, factory personnel are involved to ensure that designs meet Design for Excellence (DFX) requirements. In the production phase, defective products are analyzed and corrective actions are implemented to reduce manufacturing risks. In the verification phase, product functionality, compatibility, and reliability are tested to ensure compliance with international and environmental standards.

Risk Reporting Mechanism

In addition to actively promoting employee awareness of risk, Wistron has clearly defined its organizational structure and role responsibilities, ensuring that all employees are integrated into the risk management framework. Employees can report potential risks through various channels, including the "President's Mailbox," "Employee Opinion Box," "Employee Complaint Hotline," and "On-site Interviews with Production Line Counselors," to help mitigate the impact of internal and external risks. The Company has also revised its "Implementation Guidelines for Employee Rewards and Penalties" to recognize employees who propose effective risk mitigation, occupational safety, health, or environmental improvement initiatives. Recognition methods include verbal commendations, written acknowledgments, and formal awards, all of which encourage active participation in risk management efforts.





5.3.2 Information Security / Cybersecurity & Privacy Protection

Wistron's Information Security / Cybersecurity management mission is to “build a resilient, secure, and trustworthy enterprise.” The Company has established an Information Security Policy as its core guiding principle and is fully committed to driving digital transformation through the implementation of comprehensive information security management mechanisms. We focus on ensuring the integrity and availability of information processing and protecting the security of information systems, equipment, and networks. Through regular information security/cybersecurity drills and employee training programs, Wistron strives to build a comprehensive protection network to safeguard its information assets from potential threats.

ISO 20000 Information Technology Service Management System

In February 2018, Wistron achieved ISO/IEC 20000-1:2011 certification for its Information Service Management System. This certification reflects the Company’s commitment to delivering high-quality IT service management and complying with internationally recognized IT management standards, ensuring that its Information Technology Infrastructure Library (ITIL)-based operations meet expected performance standards. Wistron subsequently completed the transition to ISO/IEC 20000-1:2018 in January 2021, concurrently optimizing its information service management system and related processes to further strengthen IT governance capabilities and enhance overall service performance. Certified by SGS in 2024, the current certification is valid until February 22, 2027.

- ISO/IEC 20000 changes the approach to implementing internal or outsourced IT services. Implementation Benefits:
- Achieved international best practices in IT management
- IT service delivery is aligned with business objectives
- Integration of personnel, processes, and technologies to support company objectives
- Utilization of control measures for evaluation and maintenance of consistent service quality
- Compatibility between ISO/IEC 20000 and the Information Technology Infrastructure Library (ITIL) facilitates continuous improvement efforts

ISO 27001 Information Security Management System

In August 2017, Wistron achieved certification for the ISO/IEC 27001:2013 Information Security Management System, adopting the Plan-Do-Check-Act (PDCA) management model in accordance with the standard. The Company conducts at least one internal audit and one external third-party audit annually, and undergoes recertification every three years to ensure the continued effectiveness of its information security management mechanisms—demonstrating a long-term commitment to Information Security / Cybersecurity. In 2024, Wistron updated its certification to the ISO/IEC 27001:2022 version. Certified by SGS, the current certificate is valid until August 22, 2026.

- Wistron's headquarters (located in the Neihu and Xizhi office areas), the Hsinchu plant, and all overseas manufacturing plants have obtained ISO/IEC 27001:2013 verification for critical infrastructure and essential information systems necessary for continuous operations. In 2022, all manufacturing plants achieved ISO/IEC 27001:2013 certification, covering 100% of the facilities.
- In August 2024, Wistron’s headquarters (Neihu and Xizhi offices), Hsinchu site, and all overseas manufacturing sites completed the full transition to the ISO/IEC 27001:2022 certification. Coverage rate 100%.

Note: Sites sharing a data center do not have independent certification.





Information Security Policy and Organization

To effectively implement the ISO/IEC 27001 Information Security Management System, Wistron focuses on integrating procedural systems, ensuring regulatory compliance, providing personnel training, and utilizing technological applications to enhance the protection of data, information systems, equipment, and network communications. Through effective management, Wistron aims to reduce the risks of information asset theft, misuse, leakage, tampering, or destruction due to human error, malicious actions, or natural disasters, thereby fulfilling its commitments to shareholders and customers, and ensuring business continuity and operational stability.

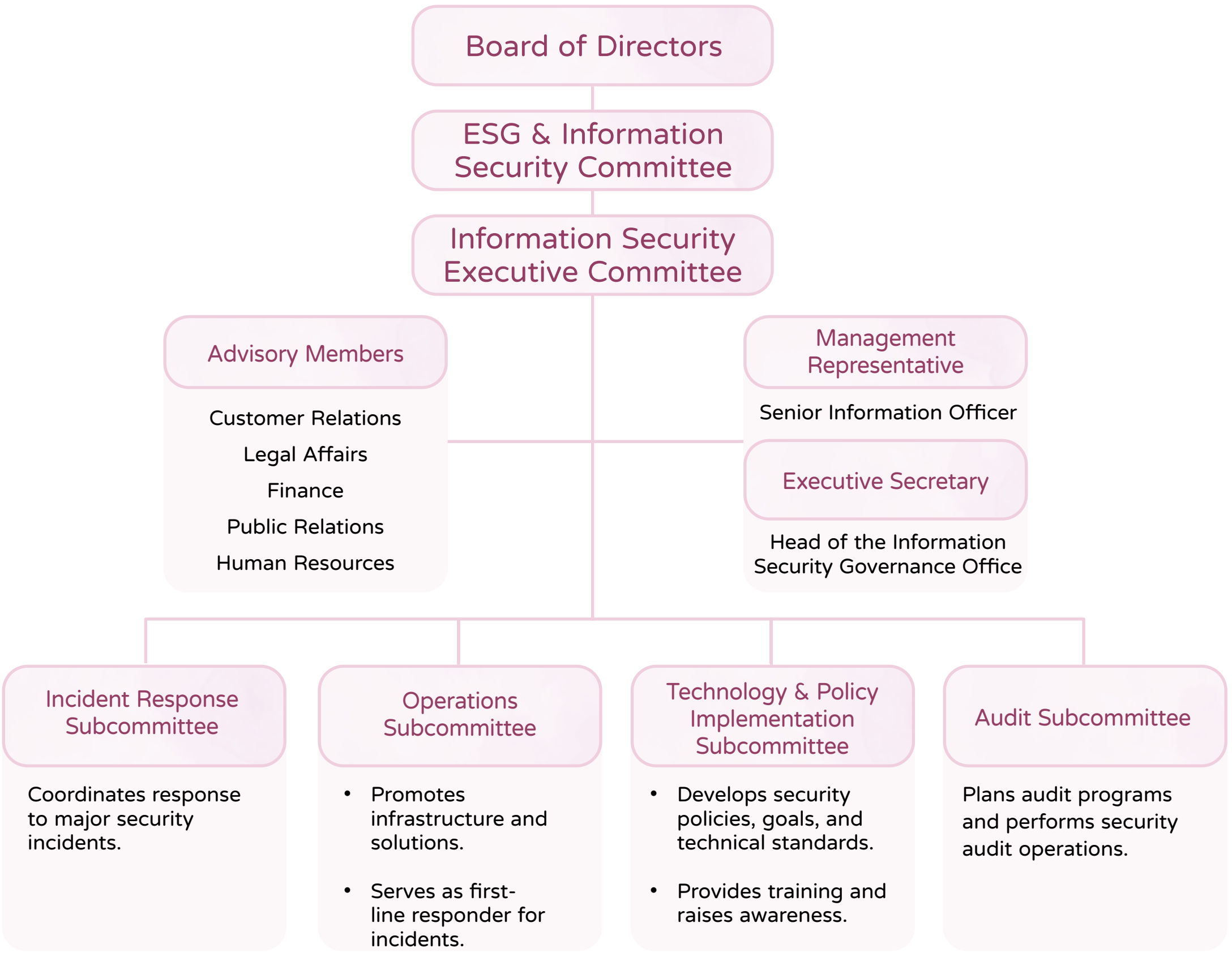
To strengthen the company’s long-term competitiveness and enhance information security governance, Wistron’s Board of Directors approved the renaming of the “ESG Committee” to the “ESG and Information Security Committee” on April 2, 2025. Under this committee, an Information Security Executive Committee was established, comprising the President & CEO, Chief Operating Officer & CTO, and Chief Digital & Information Security Officer, underscoring the Company’s commitment to cybersecurity oversight. This committee supervises the implementation of Wistron’s information security systems, technical standards, and operational practices. Wistron appointed the Vice President of Information Technology as the Management Representative, and the Head of the Information Security Governance Office as the Executive Secretary, to coordinate information security/cybersecurity affairs across the company. Wistron has established an Information Security/Cybersecurity Policy to serve as the foundation for protecting the information assets of employees, customers, suppliers, and business operations, ensuring the Company’s sustainable development.

Information Security/Cybersecurity Policy

To protect Wistron’s information, products and services, avoid unauthorized access, modification, use and disclosure, as well as losses caused by natural disasters, and provide complete and available information in a timely manner, Wistron is committed to information security/cybersecurity management to ensure the confidentiality, integrity, and availability of important information property and comply with the requirements of relevant laws and regulations, thereby gaining customer trust, meeting commitments to shareholders, and ensuring uninterrupted business operations. For more details, please refer to [Wistron Information Security/Cybersecurity Policy](#)

Information Security Executive Committee Structure

The Information Security Executive Committee (formerly the Information Security Committee) convenes on a quarterly basis. Ad hoc meetings may be convened when necessary, and members of the teams are required to attend. The meeting agenda includes information security incident reports, the report from each team on the implementation of their affairs, issues that require the cooperation of different units, other related suggestions, and extemporaneous motions. A total of four meetings were held by the Information Security Committee in 2024, and the management representative reported the information security/cybersecurity implementation status to the Board in December.

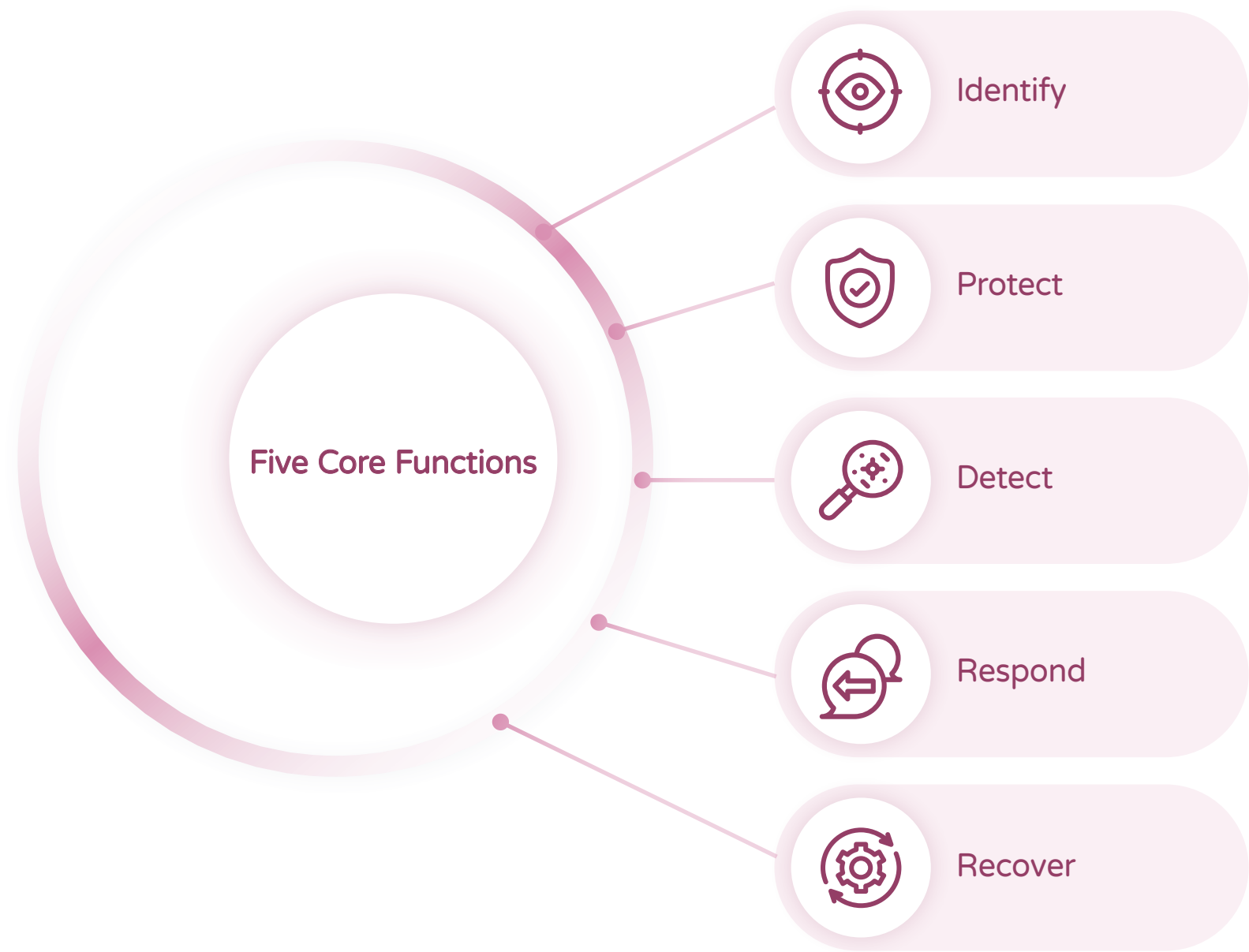




Information Security/Cybersecurity Management Strategies

To address the rapidly changing internal and external environment, Wistron has established a dedicated information security organization responsible for the planning, implementation, and risk management of information security/cybersecurity policies. Focusing on three major areas—Information Technology (IT) security, Operational Technology (OT) security, and cloud security—Wistron continuously enhances system protection, data security, and operational stability through a robust internal cybersecurity framework. Wistron also actively participates in cybersecurity intelligence-sharing platforms, including the High-Tech Cyber Security Alliance and the Taiwan Computer Emergency Response Team/Coordination Center (TWCERT/CC), to obtain the latest security alerts, threat intelligence, and vulnerability information, enabling the company to quickly identify potential risks and deploy preventive measures in advance.

Wistron utilizes the Cybersecurity Framework (CSF) stipulated by the National Institute of Standards and Technology (NIST). We evaluate the overall information security maturity and plan development blueprints for information security. We determine the priority of each matter and allocate resources accordingly, making rolling adjustments to continually strengthen and improve our systems. The framework provides the five key functions of identification, protection, detection, adaptation, and recovery. The functions include management measures for every stage of an attack against the Company, that is, pre-incident (identification and protection), during the incident (detection and adaptation), and post-incident (recovery). In the future, information security/cybersecurity is based on the Zero Trust Architecture (ZTA), which requires that every user, device, and application must undergo identity authentication and obtain authorization before accessing network systems or assets. The scope of information security/cybersecurity protection will be further extended to cloud cybersecurity (including public cloud and private cloud) and operational technology (OT) cybersecurity. We will also introduce related cybersecurity standards and assessment models, such as Cybersecurity Capability Maturity Model (C2M2), CSA Consensus Assessments Initiative Questionnaire (CSA CAIQ), and ISO/IEC 62443. As such, we assure that our overall cloud cybersecurity and operational technology cybersecurity defense capabilities will be further strengthened in the future. In response to emerging risks associated with generative AI, Wistron has enhanced its AI governance mechanisms by integrating cybersecurity governance frameworks and protection measures. Guided by the vision of Sustainability through Innovation, the Company continues to advance digital transformation, striving to build a resilient, secure, and trustworthy enterprise.



Information Security/Cybersecurity Operation Measures

- Identify stakeholder groups associated with the information security/cybersecurity management system and regularly verify the needs of stakeholder groups for the information security management system (incl. customer demands for information security).
- Carry out social engineering drills and information security training for our employees to fully increase their information security awareness.
- Establish comprehensive and clear operating procedures to institutionalize the operations of the information security management system.
- Perform regular risk assessments to identify high-risk items and invest appropriate resources to reduce or transfer risks.
- Use tools and technologies to achieve timely and effective identification, defense, detection, adaptability, and recovery.
- Establish operating procedures for response and recovery in the event of information security/cybersecurity anomalies with the aim of rapid isolation of information security incidents, elimination of threats, and reduction of the scope and extent of impact.
- Perform regular disaster recovery exercises for key applications to ensure their effectiveness.
- Perform regular annual internal and external audits each year to review the entire management system and ensure normal operation and continuous improvement.
- Pay attention to new information security developments and technologies, and update defense or management practices to effectively block new forms of information security threats and reduce risks to operations.



Information Security/Cybersecurity Management Plan

Information Security/Cybersecurity Management and Audit Mechanisms

In order to protect the Company’s intellectual property (including confidential information) and confidential customer information, Wistron has conducted multiple self-assessments and external third-party audits annually since 2017. For self-evaluations, we follow the NIST Cybersecurity Framework (CSF) and ISO/IEC 27001 standards. For external third-party audits, we comply with ISO/IEC 27001 standards and our customers’ information security requirements. These audit activities aim to ensure the effectiveness and continuous improvement of information security measures, while also strengthening internal information protection mechanisms. To support business unit development and enhance industrial control system (ICS) security, Wistron’s headquarters and Kunshan site in China successfully obtained certifications for the international automotive cybersecurity standard ISO/IEC 21434 verified by TUV (TÜV Rheinland) and the European automotive cybersecurity standard TISAX certified by SGS, in 2024, further advancing the Company’s information security/cybersecurity capabilities in the automotive sector.

Wistron actively reinforces internal control mechanisms through self-assessments conducted by operational units, in conjunction with audits by the Information Security Governance Office and the Audit Department, as part of a three-line defense. This ensures the effective implementation and continuous improvement of information security measures across all sites. In July and December 2024, operational units conducted comprehensive self-assessments using the Internal Control System (ICS), reviewing the computerized information system cycle and 11 sub-cycles. The review encompassed information systems and security policies, organizational structures, and the effectiveness of control measures in design and implementation. In June, the Information Security Governance Office completed an internal audit in alignment with the ISO/IEC 27001 transition, with no major nonconformities identified. In May, the Audit Office conducted a review in accordance with the “Internal Audit Implementation Guidelines,” focusing on information systems and security risks. The audit assessed the appropriateness of internal control systems, the implementation of general operating procedures, and specific audit projects. No major internal control deficiencies were found. In 2023 and 2024, Wistron received the Taiwan Corporate Sustainability Award (TCSA) Information Security Leadership Award for two consecutive years. In 2024, Wistron won the Information Security Governance Excellence Award at the IT Awards of Taiwan Inspection Technology Corporation (SGS), demonstrating the Company’s exemplary role and leadership position in information security management across the industry.

Supplier Chain Information Security Risk Management

In terms of supplier information security management, Wistron follows the Information Vendor Risk Management (VRM) process to classify and tier vendors, assessing their information security management life cycle from the perspectives of security, risk, and privacy. The life cycle covers the procurement phase (tier assessment, risk score assessment, contract), ongoing third-party risk management (risk score assessment and remediation), and the eventual offboarding. A total of 275 vendors were identified in 2024. Vendors were classified into tiers based on risk factors such as the importance of the services they provide, their relevance to customers and revenue, and their ability to directly access the Company’s network environment and confidential information. Vendors are classified into three tiers, with Tier 1 and Tier 2 vendors—those with higher risk levels—required to meet Wistron’s information security assessment standards based on their respective levels of risk tolerance. Our risk score assessment identified nine vendors that comply with Wistron’s information security standards.



Strengthen Employee Information Security Awareness

To strengthen employee awareness of information security/cybersecurity, Wistron actively promotes cybersecurity education and training programs. Through a combination of online and in-person courses, the Company covers topics such as general information security awareness, the “Information Security/Cybersecurity Essentials” series, and phishing email identification and prevention, helping employees understand fundamental security concepts and practical applications. In 2024, a total of 24,337 training completions were recorded, amounting to 21,346 training hours. Additionally, disciplinary actions were taken for 46 incidents involving violations of information security/cybersecurity policies, reinforcing the importance of cybersecurity.

To enhance overall information security/cybersecurity management and respond to increasingly complex cybersecurity challenges, Wistron launched the Technical Competency Model (TCM) in 2021 to ensure that its cybersecurity personnel possess the necessary skills and knowledge. Based on workforce assessments, the program defines four key roles—Security Governance, Security Engineering, Security Analysis, and Secure Software Development—each with five competency levels. Annual capability assessments are conducted to inform targeted development and advancement plans, ensuring that talent continues to evolve in line with advancements in the cybersecurity field. By 2024, a total of 89 employees—including 26 dedicated cybersecurity personnel—had joined the program, demonstrating Wistron’s strong commitment and continued investment in cybersecurity talent development.

To further enhance the professional capabilities of its cybersecurity team, Wistron encourages employees to participate in security conferences and related training programs. In 2024, the information security/cybersecurity team completed 1,599 training sessions, totaling 7,850 training hours. These included six core cybersecurity courses, five secure software development courses, and various international certification programs, such as EC-Council CEH (Certified Ethical Hacker), CISSP (Certified Information Systems Security Professional), CISM (Certified Information Security Manager), CISA (Certified Information Systems Auditor), and CompTIA certifications. These programs have not only strengthened the team's technical expertise but also enhanced its ability to address a wide range of cybersecurity threats, thereby improving the company’s overall defense capabilities.

The implementation of this program aims to ensure that Wistron remains equipped to meet rapidly evolving cybersecurity challenges, safeguard its information assets, and increase employees’ awareness and responsiveness to information security/cybersecurity risks, maintaining a competitive advantage in the field. To educate employees on information security/cybersecurity, the Company provides e-Learning resources and holds social engineering exercises every six months on phishing email simulations, reviews of employee information security

awareness, and information security education and training. In addition, the Company publishes cybersecurity e-newsletter every month to enhance our employees' awareness and vigilance of cybersecurity. The e-newsletter covers the latest cybersecurity trends and recent major cybersecurity events at home and abroad. To mitigate information security/cybersecurity risks and minimize its potential impacts, employee violations against our Information Security Policy will result in penalties according to the "Implementation Guidelines for Employee Rewards and Penalties" and be factored into their performance evaluations.

2021-2024 Phishing Click Rates from Social Engineering Drills at Wistron

Initiatives	Objectives	2021	2022	2023	2024
Social engineering drills every six months	<15% phishing click rate from social engineering drills	H1 : 10.8%	H1 : 9.3%	H1 : 7.4%	H1 : 7.8%
		H2 : 10.7%	H2 : 10.2%	H2 : 8.2%	H2 : 12.6%





Vulnerability Detection for Networks and Systems

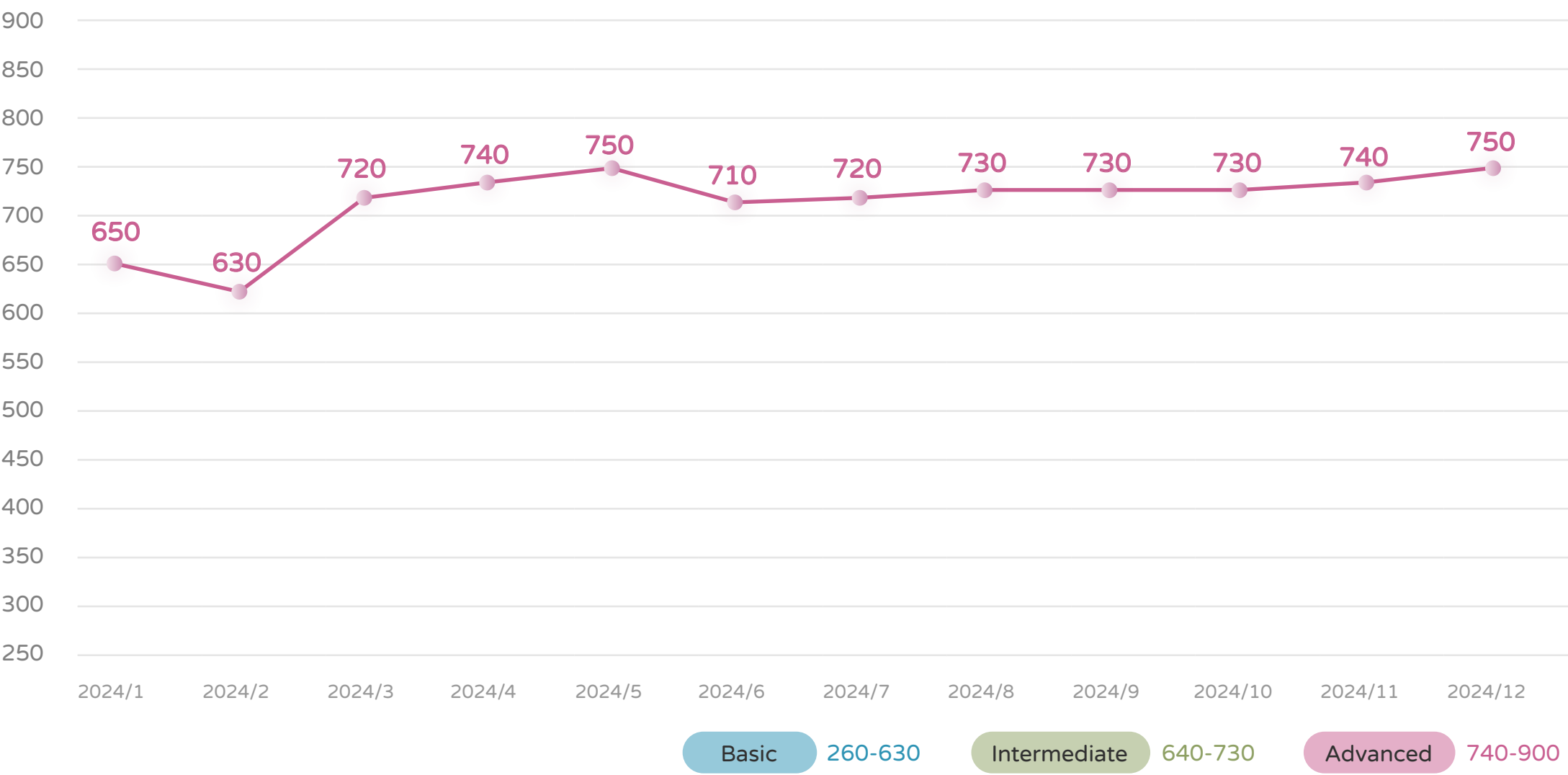
Apart from monthly internal vulnerability scans, Wistron entrusts a third-party professional organization to conduct network and system penetration tests each year to protect Wistron’s corporate and personal information and prevent losses caused by leaks, theft, destruction, other human factors, or natural disasters. These tests reduce the impact of human factors or natural factors on the Company's operations. The purpose of the tests is to understand and evaluate the status of the organization network environment and system security and verify the current information security protection safety rating and effectiveness to resolve vulnerabilities, improve operations, and strengthen system security. In 2021, we introduced red team drills, where external information security teams simulated attacks on the Company and attempted to achieve specified goals without affecting the Company’s operations. The red team drills allow us to comprehensively review our services and networks for any vulnerabilities and human errors in deployment. Moreover, we checked the integrity of identification, protection, detection, and response mechanisms from our information security maintenance and response team.

In 2024, Wistron Corporation achieved an average score of 717 in its third-party cybersecurity assessment. External evaluation enabled timely adjustments and reinforcements of network and service vulnerabilities.



2024 Wistron Corporation Third-Party Cybersecurity Assessment Results

Wistron’s 12-Month Average Score= **717** / Industry Benchmark (Manufacturing Sector)= **660-770**



Software Development Security

In order to control the security of the software development lifecycle (SDLC) and achieve "shift left" security to thereby reduce the operational costs associated with application security and maintenance, Wistron has adopted the DevSecOps (Development, Security, and Operations) mechanism. This approach enhances collaboration among the development, operations, and information security teams. Additionally, Wistron has adopted the DevSecOps Maturity Model (DOSMM) from the non-profit organization OWASP (Open Web Application Security Project) to assess the overall maturity of software development practices. This ensures that the software released meets predefined information security maturity standards. Furthermore, the incorporation of Software Composition Analysis (SCA) technology into the development workflow enhances the security quality of the software.



Information Security Alerts and Incident Management

To ensure the effectiveness of information security/cybersecurity management and enable prompt handling of security incidents, vulnerabilities, or suspicious activities, Wistron has established a comprehensive information security escalation process. This allows employees to immediately report issues and activate response mechanisms upon detection. Employees can report suspicious behavior, vulnerabilities, or security incidents to the responsible personnel through various channels, including internal platforms such as the local IT helpdesk (ext. 11119), reporting systems, or by directly contacting the Information Security team. This process ensures that every security incident receives timely attention and that appropriate response measures are initiated without delay.

To enhance rapid response and continuous protection against security incidents, Wistron has implemented an Advanced Persistent Threat (APT) monitoring mechanism, which plays a critical role in the operations of its Security Operations Center (SOC). The SOC integrates resources from both internal cybersecurity specialists and external experts to conduct 24/7 continuous monitoring and detection of potential security threats. This setup enables comprehensive oversight of the enterprise’s network security posture and related alerts, allowing timely identification and mitigation of threats and preventing the escalation of security incidents.

Regardless of the incident reported by employees or monitored by the system, according to the Wistron Information Security Incident Management Specification, information security incidents are divided into 6 levels, assessed based on the severity of 3 types of accidents, mobilize 3 different levels of response organizations, and also set the timeliness of handling and report update frequency. Each incident response process follows nine steps: initial notification and assessment/classification, escalation, initial containment, analysis, post-analysis containment, eradication, recovery, reporting and post-event experience inheritance,

this process ensures the reporting, classification, handling, institutionalized statistics and tracking, so as to quickly report and deal with the occurrence of information security incidents, and reply in the shortest possible time to ensure the normal operation of various businesses.

Business Continuity Management and Disaster Recovery Drills

To ensure the continuity of operations and critical business functions while minimizing the impact of major disaster events on key information systems, Wistron has established a comprehensive Information Security Business Continuity Plan. This plan is designed to address various unexpected situations and ensure the rapid and effective recovery of critical application systems in the event of information security/cybersecurity incidents or natural disasters, thereby preventing operational disruptions. According to the plan, Wistron conducts at least one test every six months through tabletop exercises simulating the Business Continuity Plan or Cybersecurity Incident Response Plan. These drills simulate potential cyber threats or disaster scenarios to verify the feasibility of the response plan. Through these regular tests, Wistron is able to effectively identify potential vulnerabilities, enhance response capabilities, and reduce the risk of operational disruption. In addition to drills, Wistron conducts at least one annual backup data restoration test to verify the readability of backup data, the availability of storage media, and the feasibility of recovery procedures for critical assets. These tests ensure that all data can be successfully restored within the designated timeframe, thereby reducing system recovery time and safeguarding business continuity.

The global IT center also selected 18.95% of backup storage media for seven key functional systems and databases in 2024. Recovery testing was successfully completed for the backup data. The annual global computer center disaster recovery drills revealed that the maximum tolerable data loss time during disasters (Recovery Point Objective, RPO) is 0.6 hours. After a disaster occurs, the maximum tolerable information service recovery time (Recovery Time Objective, RTO) is 19.22 hours. The results of the drills in the last four years have met the Company’s targets, and details can be found in the table below.

Strategy	Objectives	2021 Results	2022 Results	2023 Results	2024 Results
Annual disaster recovery simulations for key applications and systems to ensure continued operations and the uninterrupted provision of Company services.	RPO of SC2 Services ≤ 4 hours	RPO=0.8 hour	RPO=0.9 hour	RPO=1.0 hour	RPO=0.6 hour
	RTO of SC2 Services ≤ 24 hours	RTO=22.0 hours	RTO=18.83 hours	RTO=22.11 hours	RTO=19.22 hours
Note: 1. RPO: Recovery Point Objective (maximum tolerable data loss time in the event of a disaster) 2. RTO: Recovery Time Objective (maximum tolerable time to restore information services after a disaster)					



Information Security Insurance Mitigates Information Security Risks

In 2021, Wistron purchased global information security insurance policies as a group. Apart from mitigating risks, we also hope to further receive the help and resources of external information security experts through the international insurance market, leveraging their preventative solutions to strengthen existing information security/cybersecurity measures so that we may respond to growing information security threats and achieve corporate sustainable management.

Information Security Incidents in Past Four Years

In 2024, Wistron experienced two major information security incidents. The first occurred on March 25, when a fire at the Hsinchu site in Taiwan caused a power outage in the server room. The second took place on October 4, when the Company’s official website was targeted by a Distributed Denial of Service (DDoS) attack. In response to the cyberattack, defense mechanisms were immediately activated. There was no significant impact on business operations, and no leakage of personal data or internal documents was identified.

Number of information security violations and fines/year	2021	2022	2023	2024
Number of information security or network security violations	0	0	0	2
Data leak incidents (no. of cases)	0	0	0	0
Number of information security violations that involve customer information	0	0	0	0
Number of customers and employees affected by the data leak	0	0	0	0
Amount of fines for information security/cybersecurity or network security related incidents (NTD)	0	0	0	0

Privacy Protection

To implement personal data protection and management, Wistron formulated its [Privacy Policy](#) with reference to the laws and regulations of the jurisdictions in which it operates, and in alignment with the relevant requirements of the European Union’s General Data Protection Regulation (GDPR) as the highest guiding principle for privacy protection. The policy applies to all personnel of Wistron, Wistron’s subsidiaries and joint ventures over which Wistron has significant influence, as well as suppliers, contractors, external consultants, and other third-party partners. The policy outlines clear specifications and requirements for the use and protection of personal data, as well as related matters. All internal personnel and third-party partners are required to strictly adhere to the policy to ensure the security of personal data and protect the rights and interests of relevant stakeholders.

Wistron incorporates privacy and personal data protection into its Enterprise Risk Management systems and promotes related management actions in accordance with the [Risk Management Policy and Procedures](#) to reduce operational risks and potential impacts. In addition, the Internal Control Department conducts an internal audit project every six months through the Internal Control System (ICS) to review the collection, processing, and transfer of personal data, ensuring that all operations comply with local regulations and internal Code of Conduct.

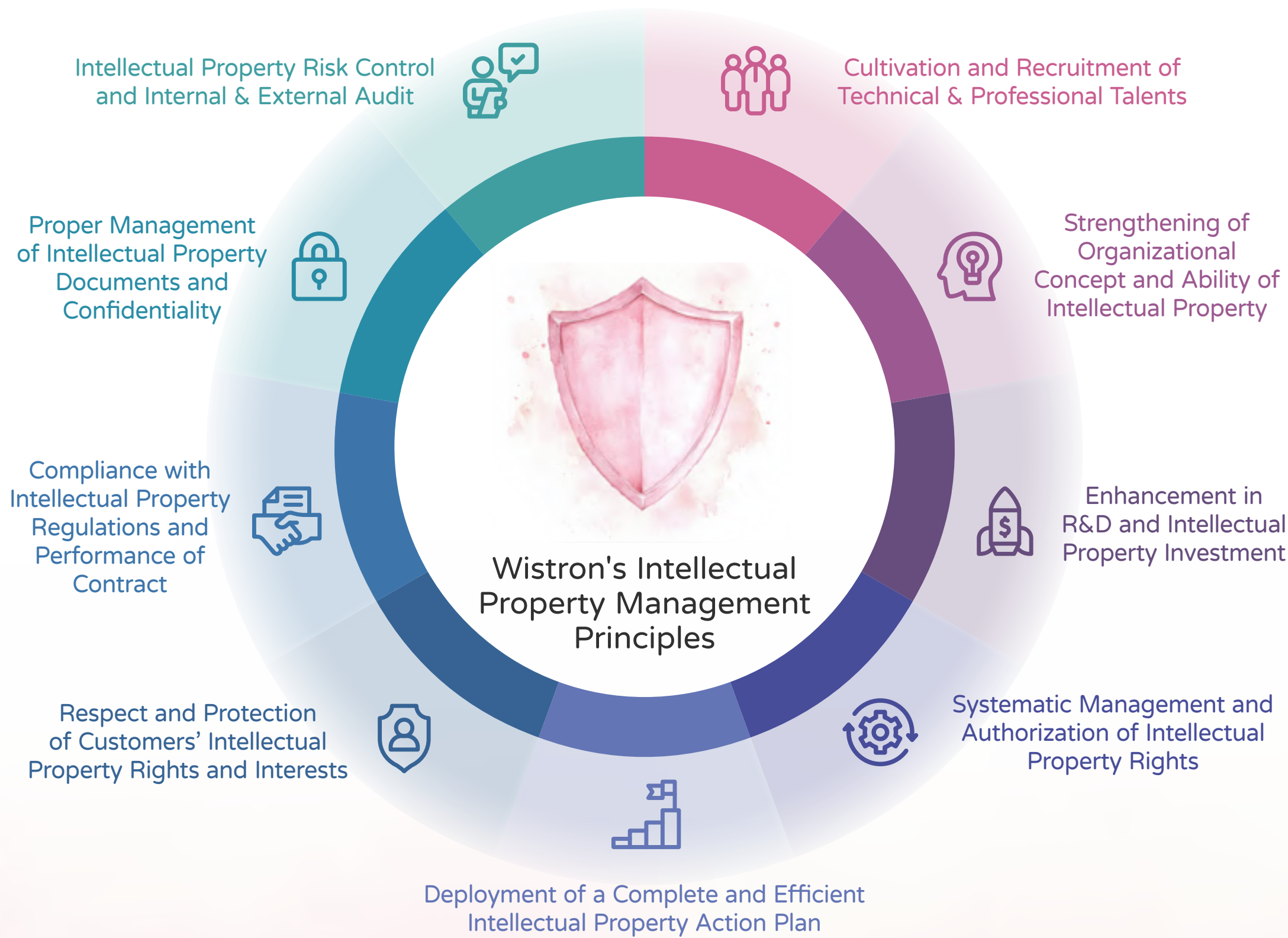
Wistron has established complaint channels for privacy-related incidents. If anyone discovers or suspects a violation of privacy rights or a breach of the policy, they may report the issue through the Privacy Protection Hotline at (02) 6616-9999 ext. 25740 or via email at ethic@wistron.com. We adopt a zero-tolerance policy toward privacy violations. Any individual found in breach of this policy will be subject to disciplinary action in accordance with the relevant provisions of the Code of Conduct, ensuring the rigor of personal data management procedures.

To strengthen privacy awareness, Wistron promotes its Privacy Policy and emphasizes its importance across global operating sites through internal electronic bulletin boards, emails, physical notices, and other communication channels. In addition, starting from the second quarter of 2024, Wistron launched the “Privacy and Data Protection Awareness” training for all employees across 25 global operating sites in 10 languages. A total of 17,886 employees completed the training, achieving a 100% coverage rate and further enhancing employee awareness and compliance with personal data management practices.

“Strictly guarding customer confidentiality and upholding the principle of integrity” is Wistron’s core commitment to customer privacy. We strictly adhere to our Privacy Policy and ensure that customer data is never used for secondary purposes (0%), safeguarding the confidentiality of all information. From 2021 to 2024, Wistron has not received any privacy-related complaints or penalties from regulatory authorities or external parties, demonstrating our rigorous management and consistent implementation of personal data protection practices.

5.3.3 Intellectual Property

Wistron places great importance on the management of intellectual capital. Through the implementation of the intellectual property rights management policy, we have strengthened our R&D capabilities, promoted high-value-added innovative products and technical services, and improved manufacturing efficiency and quality. These efforts contribute to building a forward-looking intellectual property portfolio (IP portfolio) that enhances the Company’s overall competitiveness. In the future, Wistron will continue to implement its consistent intellectual capital management plan by aligning it with the Company’s strategic considerations and operational goals to ensure the timely creation, management, and utilization of intellectual property rights.



Patent Portfolio Management

Wistron is committed to building a robust and efficient global patent portfolio. Through a well-defined patent strategy, the Company ensures that its technological achievements are protected while safeguarding the interests of its customers. To date, Wistron holds over 6,000 multinational patents. This strong patent portfolio enhances technological competitiveness and secures a market advantage for its innovations.

In terms of patent management, Wistron integrates its overall corporate strategy and business development objectives to actively drive innovation and patent deployment, ensuring the maximization of patent value. The patent team works closely with the R&D departments through brainstorming sessions, patent big data analysis, and proposal review mechanisms to identify high-quality ideas and generate goal-oriented invention proposals. Additionally, the team applies over 300 evaluation criteria to rigorously review patent specifications, ensuring that every patent meets high-quality standards. The end-to-end process—from invention proposal, patent search, scope design, drafting and translation, filing strategy, and response, to post-grant maintenance and management—is designed to ensure that Wistron’s patent assets maintain long-term competitive advantages.

To enhance the professional capabilities of patent talent and broaden employees’ understanding of intellectual property, Wistron strengthens internal professional training and has established an incentive system for inventive contributions. This reward and recognition mechanism motivates employees to innovate, further enhancing the quality and market competitiveness of Wistron’s products and technical services.

In terms of patent quantity and quality management, Wistron continues to pursue independent innovation and patent development, while also engaging in patent acquisition, investment, and the elimination of invalid patents to optimize the patent portfolio. With a consistent evaluation framework, Wistron maintains comprehensive oversight of patent coverage and market value. The Company also uses benchmarking metrics provided by third-party assessment institutions to compare its portfolio with international competitors and industry leaders, further enhancing patent competitiveness and maximizing the commercial value of its patent portfolio.



Patent Risk Management

- 1

Sophisticated intellectual property Rights Management Policy, for preventing enhanced damages from willful infringement.
- 2

Independent R&D and work-around capabilities
- 3

Strong and robust global patent portfolio
- 4

Respect the intellectual property rights of others
- 5

Avoid the infringement of valid patent rights of anyone
- 6

Use licensed technologies / products and / or multi-sourcing alternative
- 7

Contractual indemnification by suppliers / customers

Protection of Trade Secrets and Confidential Information

Trade secrets and confidential information are important intellectual assets for Wistron. We use various control mechanisms to ensure the protection of trade secrets and confidential information. Apart from maintaining our competitive advantage, these protected assets can drive innovation and ensure our customers' rights. No substantiated complaints concerning breaches of customer privacy or losses of customer data were received by the Company in 2024.

To protect confidential information of both Wistron and its customers, the Company utilizes cloud-based digital tools—such as encryption mechanisms, identity authentication, and access authorization features within Microsoft Office 365—to safeguard sensitive corporate documents. Meanwhile, we require confidential information and trade secret protection training for all new employees to ensure that employees fulfill our confidentiality commitments to our customers.

We have signed confidentiality agreements with our customers and related suppliers. Both parties are required to protect confidential information. In the past five years, we have signed an average of 400 to 700 confidentiality agreements every year. Customer information is handled by designated units to reduce the possibility of improper disclosure and leaks. We have also joined the Taiwan Association for Trade Secrets Protection to continue tracking changes to related laws and the industry.





5.4 Moving Towards a Sustainable Supply Chain

In Wistron’s strategic partnerships, suppliers play a critical role. We recognize that collaboration with suppliers is not only fundamental to business success but also a key enabler of the company’s sustainability goals. As such, a sustainable supply base has been identified as one of the Six Sustainability Strategies at Wistron. We integrate sustainability principles into procurement management by focusing on three key drivers: risk management, competitive advantage, and cost optimization. Our approach aligns with the ISO 20400 Sustainable Procurement Guidance and the Responsible Business Alliance (RBA) Code of Conduct, ensuring that suppliers continually improve their performance across environmental, social, and governance (ESG) dimensions.

In 2024, Wistron successfully implemented ISO 20400, embedding sustainability into its procurement policies and strategies. Centered on the six core subjects of social responsibility—organizational governance, human rights, labor practices, fair operating practices, consumer issues, and environmental protection—Wistron promotes sustainability goals at every stage through a systematic supplier management process and cross-functional collaboration.

5.4.1 Supply Chain Management Framework and Overview

Sustainable Supply Chain Strategy

Wistron values collaboration and mutual growth with its suppliers. Building on its Sustainable Procurement Policy and in response to customer expectations, Wistron has developed a comprehensive sustainable supply chain strategy. This strategy focuses on optimizing the core competitiveness of strategic suppliers, deepening regional strategic collaboration, and strengthening supply chain resilience. By implementing these strategies, Wistron enhances suppliers’ competitiveness in terms of technology, resources, and market adaptability. Regional cooperation further increases the supply chain’s agility and efficiency, ultimately enabling the establishment of a more stable, flexible, and resilient sustainable supply chain system in an increasingly dynamic global market environment.



- **Optimize Core Competitiveness of Strategic Suppliers:** Wistron has established global procurement and supplier quality management units to oversee supplier management. Built on a foundation of collaboration and mutual growth, these units manage the standards and procedures for supplier selection. They carry out risk assessments, performance evaluations, audit guidance, training programs, and organize supplier conferences to continuously optimize the core competitiveness of strategic suppliers and ensure that sustainability requirements are embedded in the daily management of the supply chain.
- **Deepen Regional & Strategic Cooperation:** In addition to continuously enhancing suppliers’ core competitiveness, Wistron focuses on developing local supply chains and green, low-carbon supply chains, which include: (1) Continuously reducing external environmental impacts and costs while prioritizing local supply chains and deepening regional strategic cooperation; (2) Implementing green, low-carbon supply chain programs and guiding high energy consuming material suppliers towards carbon reduction and net-zero targets, striving to minimize resource and energy consumption.
- **Strengthen Supply Chain Sustainable Resilience:** In response to supply chain risks, Wistron has leveraged digital transformation to establish a supplier data management platform and a supplier digital learning platform, enhancing the effectiveness of supply chain management. For our supplier data management platform, we regularly conduct supplier surveys to accelerate data collection and data analysis to identify our risks. For our supplier digital learning platform, we strengthen connections and engagement with suppliers through ad hoc training as well as immediate and consistent communication of our goals and sustainability-related information. We seek to ensure our suppliers fulfill their commitments, comply with the RBA code of conduct, and continue to improve.



Governance Structure

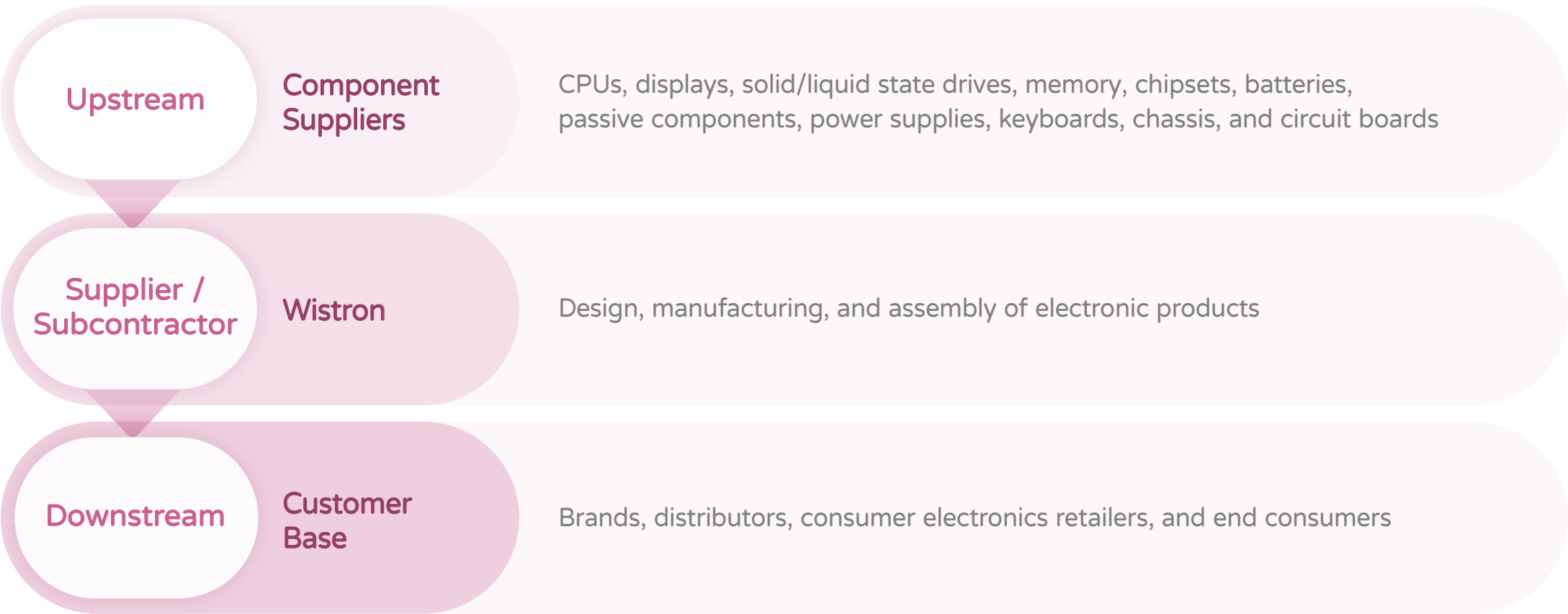
To ensure the comprehensiveness and effectiveness of sustainable supply chain management, Wistron designates the Board of Directors as the highest decision-making body for sustainable supply chain governance. The Board regularly oversees the progress and outcomes of various sustainability initiatives to ensure that all decisions and actions align with the Company’s long-term development goals. The ESG and Information Security Committee, a functional committee of the Board of Directors, reviews the work of the Sustainable supply base (pillar) twice a year to ensure the implementation of the sustainable supply chain management. In addition, the ESG Executive Committee is responsible for tracking the progress of each sustainable supply chain project and its performance results on a monthly basis.

Sustainable Supply Chain Management Organization



Wistron Value Chain

Wistron is a leading company in the global ICT (Information and Communications Technology) industry, responsible for the design, manufacturing, and assembly of electronic products, as well as related services. Positioned in the midstream of the industry value chain—with component suppliers upstream and various customer groups downstream—Wistron vertically integrates the supply chain based on customer needs and is committed to delivering competitive products that meet the diverse demands of the market and our customers.





Supply Chain Overview

As a key supplier of information technology products to the global market, Taiwan plays a vital role in the ICT industry. Rooted in Taiwan with a global outlook, Wistron leverages its strong technical capabilities to provide customers with comprehensive hardware and software solutions, along with one-stop system integration services. By establishing a worldwide network of manufacturing sites and service hubs, Wistron ensures efficient and reliable support across global markets, meeting the needs of customers in various regions and further strengthening its core position within the global supply chain.

Wistron's main suppliers fall into four major categories: electronic parts, mechanical parts, maintenance repair operation (MRO), and logistics suppliers. In 2024, Wistron engaged in transactions with 1,683 suppliers. To enhance management efficiency and strengthen collaboration with key partners, suppliers are categorized into tiers, enabling more focused and in-depth supplier management. With ongoing supply chain restructuring and adjustments to Wistron’s manufacturing sites, the supply chain has been reconfigured to ensure greater flexibility, reduce risks, and enhance supply chain stability. Tier 1 suppliers are those who have conducted more than six transactions per month and accounted for over 90% of the annual transaction amount. In 2024, there were 404 tier 1 suppliers. Based on transaction share and strategic importance, 242 of these were further identified as significant tier 1 suppliers¹ . To gradually reduce overall supply chain risks, we expanded our management scope to include non-tier 1 suppliers, identifying 171 such suppliers. Among them, 134 were further defined as significant non-tier 1 suppliers² and incorporated into our risk control measures to ensure stable supply chain operations.

2024 Supplier Distribution by County/Region

	Total Number of Suppliers	Proportion of Purchase Amount (%)
Taiwan	522	55.86
China	908	34.20
Asia Pacific	129	6.79
Americas	84	1.42
Europe	22	0.21
Others	18	1.52
Total	1,683	100

2024 Tier 1 Suppliers by Category

	Total Number of Suppliers	Proportion of Purchase Amount (%)
Electronic parts	165	60.57
Mechanical parts	204	36.13
Maintenance Repair Operation	23	1.31
Logistics	12	1.99
Total	404	100

2024 Suppliers by Classification

	Total Number of Suppliers	Proportion of Purchase Amount (%)
Tier 1 suppliers	404	94.27
Significant tier 1 suppliers	242	87
High risk suppliers	9	-
Significant non-tier 1 suppliers	134	-

Note :

1. Significant tier 1 suppliers: Including critical suppliers - high proportion of turnover (top 80% of annual transaction amount); ability of technology pioneering; the only source of supply is irreplaceable; high-risk suppliers - SAQ score below 80.

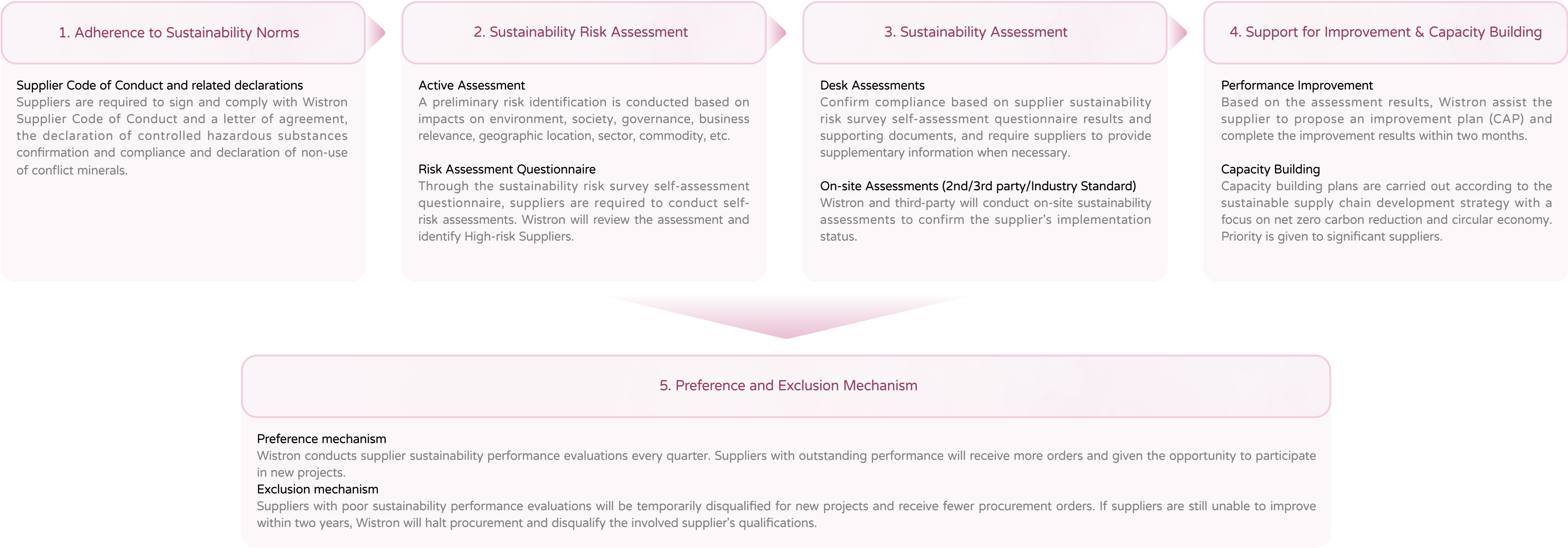
2. Significant non-tier 1 suppliers: (i) Agency transaction with SAQ score below 80 (Potentially high-risk suppliers); (ii) The upstream supplier of the customer's designated trading supplier.



5.4.2 Supply Chain Sustainability Management

Wistron has established a comprehensive sustainable supply chain management process that consists of five core steps: adherence to sustainability norms, sustainability risk assessment, sustainability assessment, improvement and capability building, and preference and exclusion mechanism. This process is designed to ensure that all suppliers fully comply with the requirements of the Supplier Code of Conduct and effectively avoid potential ESG-related conflicts. Through systematic risk assessments and audits, Wistron works closely with suppliers to verify implementation, provide guidance on areas for improvement, and assist in developing action plans. In addition, Wistron actively promotes economic inclusion and resilience-building among suppliers. Through long-term collaboration, we aim to enhance suppliers’ sustainability performance and further solidify Wistron’s critical role and impact within the supply chain.

Supplier Sustainability Management Structure





Compliance with Sustainability Standards

Supplier Code of Conduct

In advancing corporate sustainability, Wistron recognizes the critical impact of supply chain management on both society and the environment. To this end, Wistron has established a Supplier Code of Conduct as a foundation for supplier action in sustainability practices. This Code is aligned with the Responsible Business Alliance (RBA) Code of Conduct and the United Nations Guiding Principles on Business and Human Rights, covering five core areas: labor rights, health and safety, environmental protection, ethics, and management systems. The Code also includes specific requirements related to biodiversity, the prevention of deforestation, and land conservation, aiming to holistically enhance the sustainability of the supply chain. Wistron also incorporates the level of supplier compliance with the Code as a key evaluation criterion in procurement decisions to ensure alignment between supply chain partners and the Company’s sustainability goals. In 2024, 100% of Wistron’s suppliers signed the Supplier Code of Conduct, demonstrating their full recognition of and commitment to Wistron’s sustainability standards. In addition, depending on the supplier category, Wistron further required the signing of the letter of agreement, the declaration of controlled hazardous substances confirmation and compliance, and the declaration of non-use of conflict minerals, all of which also achieved a 100% signing rate. These measures have not only strengthened Wistron’s governance capabilities within the supply chain but also promoted a shared commitment among partners to uphold higher standards of social and environmental responsibility.

Signing of the Supplier Code of Conduct

Year		2024 Performance	2024 Targets
Existing suppliers	Number of suppliers required to sign	1,338 (cumulative)	-
	Percentage of signed suppliers (%)	100%	100%
New Suppliers	Number of suppliers required to sign	2	-
	Percentage of signed suppliers (%)	100%	100%

Sustainability Risk Assessment

In order to assess sustainability risks within the supply chain, Wistron conducts a two-phase risk investigation on suppliers. Through varying requirements at different stages, we aim to evaluate suppliers’ ESG performance and identify potential risks within the supply base. The first phase focuses on comprehensive risk screening, while the second phase further identifies high-risk suppliers. For high-risk suppliers identified through the assessment process, Wistron initiates an assessment procedure, combining professional guidance with support to help suppliers develop and implement improvement plans. This approach enables effective control at the source of risk and helps reduce overall sustainability risks within the supply chain.

Active Assessment
Target: All suppliers

To identify potential risks within the supply chain, Wistron conducts preliminary assessments and screening of suppliers. The evaluation covers multiple dimensions, including environmental, social, and governance (ESG) performance, business relevance, country or region of operation, industry type, and product characteristics. Through this process, suppliers with potential risks are preliminarily identified and brought under management to reduce overall supply chain risk.

Factor	Content
Environmental	<ul style="list-style-type: none">Review major negative events or illegal records related to environmental issues, including but not limited to excessive hazardous substances, air pollution emissions, water pollution emissions, improper disposal of waste and toxic substances, etc.Evaluate potential negative impact factors related to environmental issues, such as high carbon emissions, non-local procurement leading to increased energy consumption and resource waste, etc.
Social	<ul style="list-style-type: none">Review major negative events or illegal records related to social issues, such as violations of labor rights or occupational safety, forced labor, etc.Evaluate potential negative impact factors related to social issues, such as the disclosure of negative reports involving the living wage or impact on local communities.
Governance	<ul style="list-style-type: none">Review major negative events or illegal records related to governance issues, including corporate fraud, bribery or false financial reports, etc.Evaluate potential negative impact factors related to governance issues, such as insufficient operational soundness or anti-competitive behavior.
Business relevance	<ul style="list-style-type: none">For critical business categories, we conduct a preliminary assessment based on procurement amount and in consideration of the irreplaceability of products and the pioneering nature of industry technology.

Key Sustainability Risk Factors and Countermeasures for Suppliers in 2024

Factor	Content
Country / Region	<ul style="list-style-type: none">Based on the location of the supplier, we include regional and high-risk country controls and consider geopolitics, conflicts, and risk identification of high-risk countries.
Sector	<ul style="list-style-type: none">Based on industry and business attributes, we evaluate the resource intensity and labor requirements of service processes or those involving specific concerns.
Commodity	<ul style="list-style-type: none">Based on product attributes and raw material composition, we seek to have comprehensive understanding of any potentially hazardous substances or high-energy-consuming materials.

Risk Assessment

Assessment Scope: Tier 1 and non-Tier 1 Suppliers

To comprehensively understand the sustainability risks of existing suppliers, Wistron distributes a Sustainability Risk Self-Assessment Questionnaire to both Tier 1 and non-Tier 1 suppliers, requiring them to provide supporting documentation to gain deeper insights into their sustainability risks and management practices. The questionnaire covers five key sustainability dimensions: sustainability and operation risk management, supply chain and continuity operation, environmental protection, human rights and labor protection, and occupational safety and health. Through this mechanism, Wistron is able to identify and manage sustainability risks across the supply chain and mitigate potential risks.

Suppliers with a score of less than 80 are defined as high-risk suppliers. In 2024, a total of 9 high-risk suppliers were identified. According to the results, the main sustainability risk factors in 2024 were concentrated in the areas of environmental protection and sustainability and operational risk management. In order to effectively mitigate the impact of these risk factors, Wistron will prioritize greenhouse gas inventory and certifications (ISO 50001 and ISO 14064-1) for critical and high-energy-consuming material suppliers, in addition to promoting the purchase of renewable energy certificates. Other identified risk factors will be listed as items requiring guidance for remediation through assessment and improvement programs.

Dimension	Risk factors	Countermeasures
Environmental Protection	Energy conservation and carbon reduction mechanisms for energy management have not been implemented (ISO 50001)	Engaged high-energy-consuming material suppliers to obtain ISO 50001 certification
	Uncertified greenhouse gas inventory certification management (ISO 14064-1)	Engaged high-energy-consuming material suppliers to obtain ISO 14064-1 certification
	No statistics on scope 3 greenhouse gas emissions generated by products or services	Engaged high-energy-consuming material suppliers in Scope 3 greenhouse gas inventory
	Lack of green electricity or renewable energy usage	Encouraged suppliers to purchase renewable energy certificates or use solar power panels
Sustainability and operational risk management	Response plan management for business continuity has not been implemented	List as items requiring guidance for remediation



Sustainability Assessment

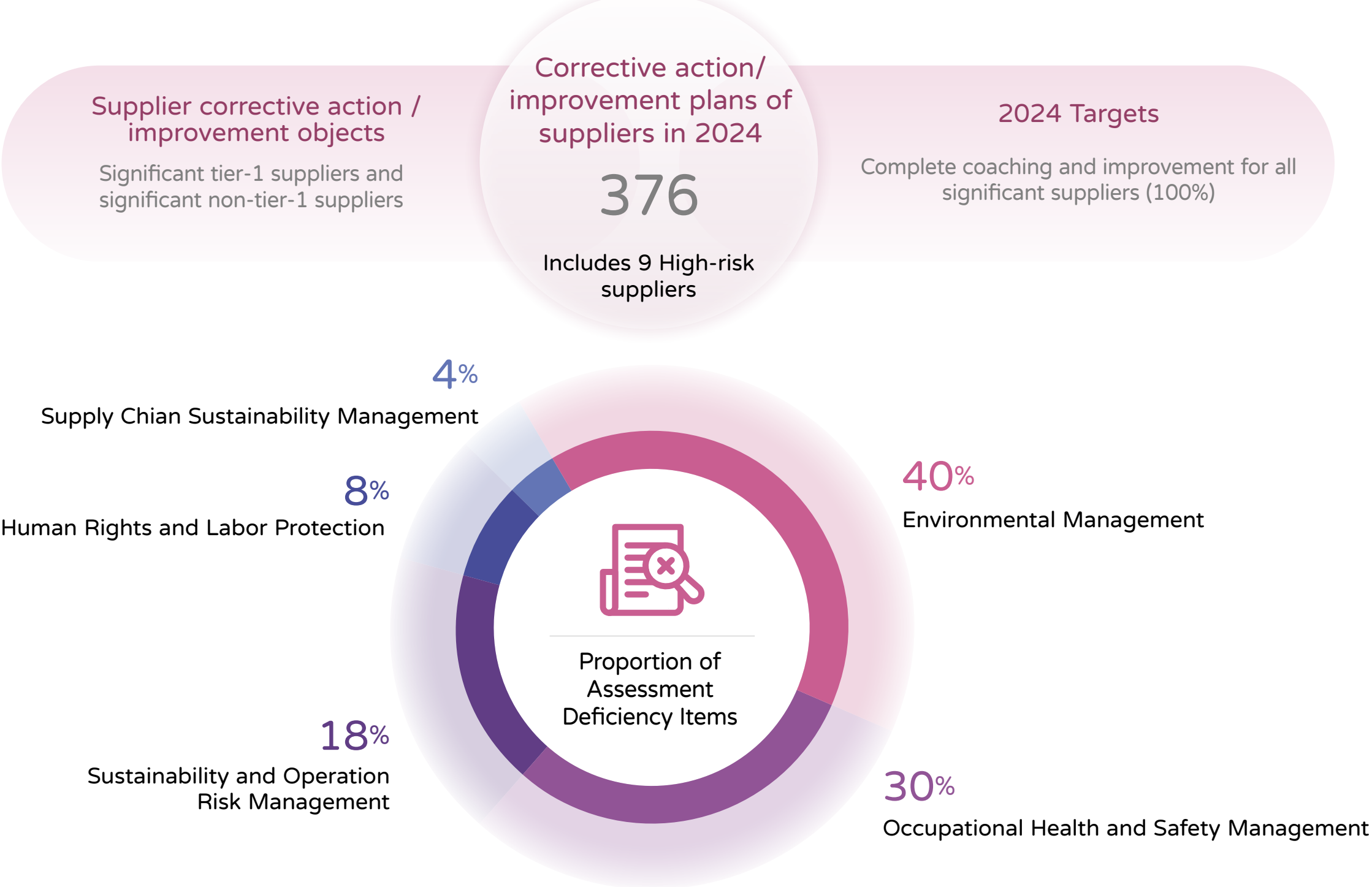
To comprehensively assess the implementation of sustainability practices among suppliers, Wistron adopts a diversified assessment approach, including both desk assessments and on-site assessments. On-site assessments are further categorized into 2nd party assessments, 3rd party assessments, and assessments conducted in accordance with industry standards. Wistron has also established annual targets and a long-term goal for 2030, providing clear direction for promoting sustainability in the supply chain over both the short and long term, thereby enabling continuous progress toward these objectives.

Type	Assessment Format	Approach	Scope	No. of Assessments in 2024	2024 Targets	2030 Targets
Desk	Desk assessments	Distribute self-assessment questionnaire on sustainability risks and request supporting materials	575 tier 1 and non-tier 1 suppliers	575	Conduct desk assessments for all significant suppliers	Conduct desk assessments for all suppliers (incl. tier 1 & non-tier 1)
On-site assessments	2nd party assessments	On-site or remote assessments and review operations are performed by Wistron for significant tier 1 suppliers, and by tier 1 suppliers or consultants for non-tier 1 suppliers	376 significant tier 1 suppliers and significant non-tier 1 suppliers	344	Conduct on site assessment for all significant suppliers	Conduct on site assessment for all significant suppliers
	3rd party assessments	Third-party verification		6		
	Industry Standard	Assessments based on RBA standards		26		
	Total number of on-site assessments			376	100%	100%



Corrective Action/Improvement Plans

To enhance the sustainability performance of suppliers, Wistron provides counseling measures for deficiencies identified in assessments, including on-site and remote support to assist suppliers in developing and implementing improvement plans. If the supplier is unable to complete the improvements within two months, they may submit another assessment application for a second assessment to confirm the implementation of the improvement plan. However, if a supplier fails to pass the second assessment, they must wait six months before reapplying. During this period, Wistron will evaluate the feasibility of using alternative materials or consider replacing the supplier. If immediate substitution is not feasible due to urgent supply requirements, the replacement will proceed once an alternative is in place. For suppliers unable to meet improvement requirements within two years, Wistron will gradually reduce procurement volume until the partnership is terminated or the supplier is disqualified. In 2024, all assessed suppliers completed the required improvements within the specified timeframe, and no partnerships were terminated due to non-compliance.



Supplier assessment corrective/improvement actions

Dimension	Topic	Corrective / Improvement actions
Sustainability and operation risk management	Operation continuity / anti-corruption policy	<ul style="list-style-type: none"> Conducting regular annual risk assessments to identify emerging corruption risks and potential threats to business continuity. Integrating anti-corruption commitments and codes of conduct into corporate policies, enhancing training content related to anti-corruption, and implementing training programs as planned. Ensuring that all employees are aware of and understand the mechanism. Establishing an anonymous whistleblowing mechanism to encourage employees and external parties to report suspected corrupt practices for timely investigation and response.
Supply chain sustainability management	Supplier selection / management	<ul style="list-style-type: none"> Developing a comprehensive risk management strategy to ensure supply chain stability and resilience. Conducting in-depth analysis to identify potential risks across all stages of the supply chain, enabling the early implementation of mitigation measures. Promoting the phased integration of suppliers into sustainable development practices to ensure the gradual achievement of environmental and social responsibility goals.
Environmental management	Energy management / Greenhouse gas management	<ul style="list-style-type: none"> Establishing an energy monitoring system, develop relevant regulations, and set clear quantitative indicators to control and optimize energy use, and implement carbon reduction plans according to defined procedures. Establishing emission reduction baselines and adopt effective technologies and methods to reduce emissions, with regular reporting on results and progress.
Human rights and labor protection	Working hours management / Non-discrimination	<ul style="list-style-type: none"> Establishing monitoring mechanisms to ensure working hour arrangements comply with legal requirements; providing training on working hour systems for employees and managers to support work-life balance. Organizing regular non-discrimination training and incorporating it into the annual training plan to ensure comprehensive employee education. Systematically maintaining training records and incorporating them into progress and effectiveness tracking.
Occupational health and safety management	Emergency preparedness / Chemicals management	<ul style="list-style-type: none"> Providing targeted safety training programs based on the specific risks associated with different job positions to ensure all employees have the necessary safety knowledge and skills. Developing detailed emergency response plans with clearly defined responsibilities, and conducting regular drills for fire, earthquake, and chemical incidents to enhance employee response capabilities. Enhancing and upgrading safety protection facilities, and regularly reviewing chemical safety data sheets to ensure chemical management complies with safety standards.



Preference and Exclusion Mechanism

To encourage suppliers to implement sustainable practices and enhance their sustainability performance, Wistron conducts sustainability performance evaluations of suppliers and implements a preference and exclusion mechanism in accordance with relevant management procedures.

- Preference: Suppliers with outstanding sustainability performance ratings are prioritized as primary suppliers, receive higher order allocations, and are granted opportunities to participate in new projects. They are also recognized and honored as Outstanding Suppliers during the annual Partner Conference, with a total of 11 suppliers recognized in 2024. In 2024, a total of 6 suppliers received increased orders due to the preference mechanism.
- Exclusion: Suppliers with poor sustainability performance ratings have their eligibility for new project introductions suspended and their procurement amounts reduced. If a supplier fails to improve their performance within a two-year period, their procurement is halted, and their supplier status is revoked. In 2024, no suppliers met the criteria for exclusion.

Supplier Sustainability Evaluation

Wistron has established ESG-related thresholds for all suppliers, including both new and existing ones. To become a qualified Wistron supplier, vendors are required not only to sign the Code of Conduct but also to obtain certifications such as ISO 9001, ISO 14001, IECQ QC 080000, and ISO 45001.

For new suppliers, Wistron conducts evaluations using the supplier quality system evaluation form, in which ESG factors account for 13.33% of the total score. These factors include:

1. Establishing appropriate and effective documents and procedures related to the RBA Code of Conduct
2. Compliance with labor standards
3. Compliance with health and safety standards
4. Compliance with environmental standards
5. Compliance with ethics business standards
6. Compliance with management system

Wistron evaluates the ESG performance of existing suppliers through the supplier performance evaluation. Evaluation criteria include supplier’s quality, reliability, compliance, supply capability, price, and ESG sustainability performance. Among these, ESG factors account for 20% of the total score and include:

1. Quarterly reviews of ESG sustainability activities
2. ISO 14064-1 certification annual review

3. ISO 50001 certification annual review
4. Annual ESG sustainability audit score
5. Major Missing Events of ESG Sustainability On-site Assessment
ESG risk management and mitigation plans (Human Rights: Whether the supplier conducts human rights risk assessments and if there are any reported human rights violations. Operational Risk: Whether the supplier provides financial statements or key financial indicators, and whether related risks are disclosed or addressed. Disaster Preparedness: Includes fire safety and natural disaster readiness.)





Capacity Building

Buyer Education Training

Procurement-related departments (including buyers, logistics, quality assurance, and other supply chain functions) are equipped to understand supplier management processes and their roles in sustainability. Educational training is a key element of corporate sustainable development. Through systematic courses, procurement staff enhance their understanding of environmental, social, and governance (ESG) issues, including the prohibition of forced labor (such as slavery or human trafficking). The training further focuses on building sustainability-related competencies tailored to core procurement functions, enabling staff to incorporate ESG strategies into daily operations and supplier engagement. In 2024, Wistron collaborated with the ESG Sphere Course Review Committee to develop a series of ESG-related online training modules. A total of 2,170 individuals were trained, amounting to 1,497 hours of education.

Supplier Education Training

To support suppliers in adopting ESG-aligned strategies and actions in their operations—and to strengthen the overall resilience and sustainability of the supply chain—Wistron continues to offer relevant training through its online supplier education platform. These courses aim to enhance suppliers’ understanding of sustainable development practices and reinforce partnerships based on shared ESG values. In addition to the mandatory annual training on the Supplier Code of Conduct, a new required course—Introduction to ISO 14064-1—was introduced this year to raise awareness of energy conservation and carbon reduction. A total of 404 Tier-1 suppliers completed the training, achieving a 100% completion rate.



Partner Conference and Sustainability Sharing Forum

In 2024, Wistron continued to center its efforts around Resilience – Challenges & Opportunities. At the Wistron Group Partner Conference, the company shared its achievements in sustainable resilience and its roadmap toward emission reduction targets. Leveraging the "big leads small" effect, Wistron guided its supplier partners in progressing toward the net-zero goal. The company also recognized and honored suppliers who demonstrated outstanding performance in sustainability and a strong commitment to integrity. Through these efforts, Wistron aims to cultivate a spirit of collaboration, mutual benefit, and sustainable growth across its business ecosystem.

To promote supplier engagement, Wistron hosted two Supplier Sustainability Sharing Forums in 2024:

- First forum: Topics included the RBA (Responsible Business Alliance) Code of Conduct and case studies, corporate carbon management and greenhouse gas inventory, product carbon footprint verification, and an introduction to energy management systems. Wistron also presented its sustainability management policies and communicated its requirements on anti-corruption, GHG inventory, and water risk management. In addition, the company introduced its supplier sustainability survey systems. More than 15 leading electronics suppliers shared best practices and case studies on energy-saving technology upgrades and carbon reduction measures. These exchanges aimed to help suppliers better understand the current state of industry sustainability and enhance their motivation to engage in sustainable development. A total of 283 suppliers participated.
- Second forum: The then Vice President of Intel and General Manager of Intel Taiwan was invited to share insights on “How Companies Can Build a Workplace with diversity, equity, and inclusion (DEI)”, helping suppliers understand how to foster a diverse and inclusive corporate culture. A total of 28 suppliers participated.





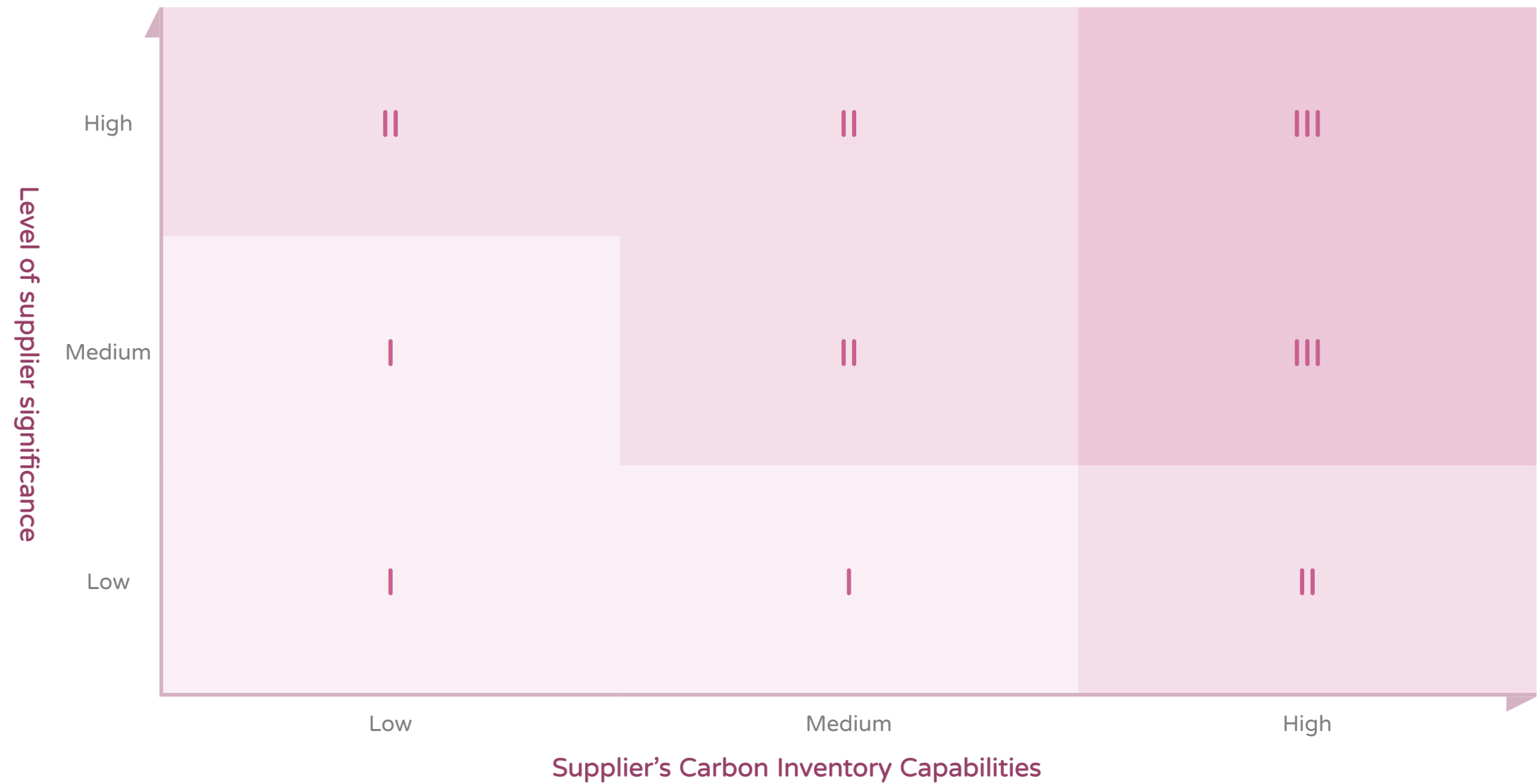
Capacity Building Project: Promoting Net Zero Carbon in the Sustainable Supply Chain

Establishing a segmented supplier carbon management promotion strategy

Starting from 2021, annual greenhouse gas inventory results from suppliers are collected. Upon analysis, it was found that suppliers exhibit varying degrees of capability in carbon inventory and reduction. Consequently, a classification management system has been implemented, categorizing suppliers based on their level of significance (determined by factors such as revenue and material substitutability) and carbon inventory capabilities. Tailored project plans are provided to suppliers in different categories, along with necessary assistance resources, experience-sharing courses, and consulting resources, to ensure their progressive advancement towards carbon neutrality.

Type	Carbon management strategies for suppliers
I	<ul style="list-style-type: none">Conduct greenhouse gas inventory and factory-side self-inventory
II	<ul style="list-style-type: none">Third-party verification for scope 1 and scope 2 GHG inventoryScope 3 GHG inventoryISO 50001 energy management system certification for high-energy-consuming material suppliersEstablish a carbon reduction project with an annual reduction of 4.2%
III	<ul style="list-style-type: none">Third-party verification for scope 1+2+3 GHG inventoryISO 50001 energy management system certification for high-energy-consuming material suppliersJoin the SBTi commitment or set up a 4.2% annual carbon reduction project

Level of supplier significance





Building supplier carbon management sustainability capabilities

Wistron conducted a comprehensive inventory of Scope 3 greenhouse gas emissions across all 15 categories, with results indicating that upstream raw material procurement accounts for the highest share of emissions. In response, Wistron launched a carbon management capacity-building program tailored to different categories of suppliers. The program covers carbon inventory training, verification mechanism enhancement, the introduction of Science Based Targets (SBTi) initiative emission reduction targets, and collaborative carbon reduction projects. In 2024, Wistron initiated four carbon management projects and engaged in in-depth collaborations—lasting over six months—with 206 significant suppliers, continuously enhancing the carbon management capabilities of supply chain partners and jointly advancing emission reduction targets.

Type	Project	Cooperative partner-Significant Suppliers	Details	Benefits & Impacts
I	Carbon inventory capacity building plan	Tier-1 suppliers (No carbon emissions inspection has been carried out)	Supported suppliers in building organizational carbon inventory capabilities through online practical training courses on greenhouse gas inventory and data verification, in collaboration with ezGreen.	6 suppliers participated in the carbon inventory course, achieving a 100% greenhouse gas data feedback rate 6 suppliers – 3 verified / GHG inventory reports and emission registers submitted x6
		Significant suppliers	Collected supplier carbon inventories to complete supply chain emission data	Completed carbon inventory data and sustainability survey for 206 suppliers
II	High energy-consuming material suppliers' verification program	High energy-consuming material suppliers	Since 2022, we have been consistently expanding our categories, selecting critical high energy-consuming material suppliers to promote ISO 14064-1 and ISO 50001 certification	Out of the 52 suppliers selected for promotion, 39 attained ISO 14064-1 certification, while 34 achieved ISO 50001 certification.
	Low-carbon transformation promotion plan	High energy- consuming material suppliers	Wistron joined government-led low-carbon transition initiatives by leveraging the “big leads small” approach, collaborating with 30 suppliers in total. Among them, Wistron worked closely with 7 suppliers to establish carbon reduction mechanisms and promote low-carbon practices. These efforts included sharing energy-saving technology improvement strategies, commissioning research institutes to conduct supplier energy audits and diagnostics, and establishing project verification mechanisms for energy conservation and carbon reduction. Technical support was also provided to promote industrial energy efficiency improvements and carbon management tools. Furthermore, Wistron works with 23 suppliers on supply chain carbon inventory and digital carbon management applications. Through a systematic approach, Wistron collects carbon information and relevant sustainability data from suppliers, enabling effective monitoring of suppliers' sustainability management status.	We collaborated with seven suppliers to jointly propose energy-saving improvement projects, resulting in approximately 21.74 million kWh of electricity saved and a cumulative reduction of 10,742 tCO2e. Completed carbon inventory and sustainability data surveys for 23 suppliers, serving as a foundation for subsequent evaluation and project analysis.
III	SBTi initiative commits to promote	Suppliers with high carbon inventory maturity	Collaborate with customers to target and encourage suppliers in high energy-consuming industries to participate in SBTi and respond to CDP questionnaires	Among 13 customer-designated suppliers, 10 have signed the SBTi commitment. An additional 20 suppliers were engaged to sign the SBTi commitment, and 30 suppliers responded to the CDP questionnaire.



Supplier capability building KPI

KPI	2024 performance	2024 Targets
Number of companies building carbon management capabilities	206 Suppliers	188 Suppliers
Proportion of Significant Suppliers (%)	54.79%	50%

Green Supply Chain Management

A green, transparent, and circular supply chain encompasses all the essential elements of a modern, sustainable supply chain. Wistron’s green supply chain management covers the following aspects:

- **Green Design:** Incorporates RoHS and Product Carbon Footprint (PCF) standards at the design stage to ensure environmental compliance.
- **Green Procurement:** Prioritizes eco-friendly materials and certified suppliers to reduce carbon footprint.
- **Green Manufacturing:** Partners with low-carbon suppliers to implement carbon reduction strategies and promote sustainable production.
- **Green Packaging:** Reduces and reuses packaging materials while ensuring reliability. Prioritize suppliers with Forest Management (FM) and Chain of Custody (CoC) certifications for shipping materials to ensure sustainable sourcing.
- **Green Transportation:** Utilizes low-emission, energy-efficient, and smart logistics solutions to support carbon reduction.
- **Green Recycling:** Promotes the use of recycled plastics and EPE; encourages reuse and resale of inventory to minimize waste. Reuse excess inventory and facilitate resale to reduce stock levels and minimize waste.

These measures ensure that every stage of the green supply chain meets environmental standards and supports the company’s progress toward sustainable development goals.

Supplier Circular Economy Project Cooperation

Amidst the global push for a circular economy, Wistron remains committed to safeguarding natural life and forests by fostering communication and collaboration with suppliers. This focus enables the fulfillment of biodiversity and non-deforestation pledges, while simultaneously reducing the Earth's environmental burden. Furthermore, it enhances suppliers' sustainability awareness and capabilities to adapt to evolving sustainability trends.

Supplier Partnership Projects	Details	Qualitative Benefit	Quantitative Benefits
Replaced internal cardboard turnover boxes with reusable plastic containers	In 2024, Wistron adopted the WT Microelectronics Smart Logistics System, utilizing recyclable turnover boxes to reduce commercial waste.	Recyclable plastic containers can be reused multiple times, reducing natural resource consumption and offering stronger environmental benefits. Resource reuse and improved disposal processes enhance overall economic efficiency and mitigate environmental impacts from production growth.	<ul style="list-style-type: none">• Using reusable plastic boxes in place of cardboard reduces the volume and weight of waste paper.• Reduced waste weight supports the achievement of waste reduction targets.• Stackable containers save space and reduce transportation costs.• Reduced procurement costs for turnover boxes, saving NTD 2,350,540 annually.• Reduced cardboard waste: 174 tons/year, disposal cost savings of NTD 469,800.• Achieving the company’s waste reduction target of 2%.
Optimized packaging materials such as dividers (cardboard and urea panels)	Partnered with suppliers to replace non-recyclable divider materials with recyclable alternatives, such as bubble wrap, to reduce packaging waste.	Strengthened supplier collaboration by jointly addressing environmental challenges, enhancing overall supply chain efficiency and innovation. Suppliers and Wistron worked together to reduce waste and lower costs.	<ul style="list-style-type: none">• Packaging changes included replacing cardboard dividers and urea panels with recyclable bubble wrap to support waste reduction targets.• Reduced total waste generation by 5,621.9 kg.• Packaging cost optimization: Recyclable bubble wrap proved more cost-effective than traditional materials, saving NTD 253,236.



5.4.3 Conflict Minerals Management

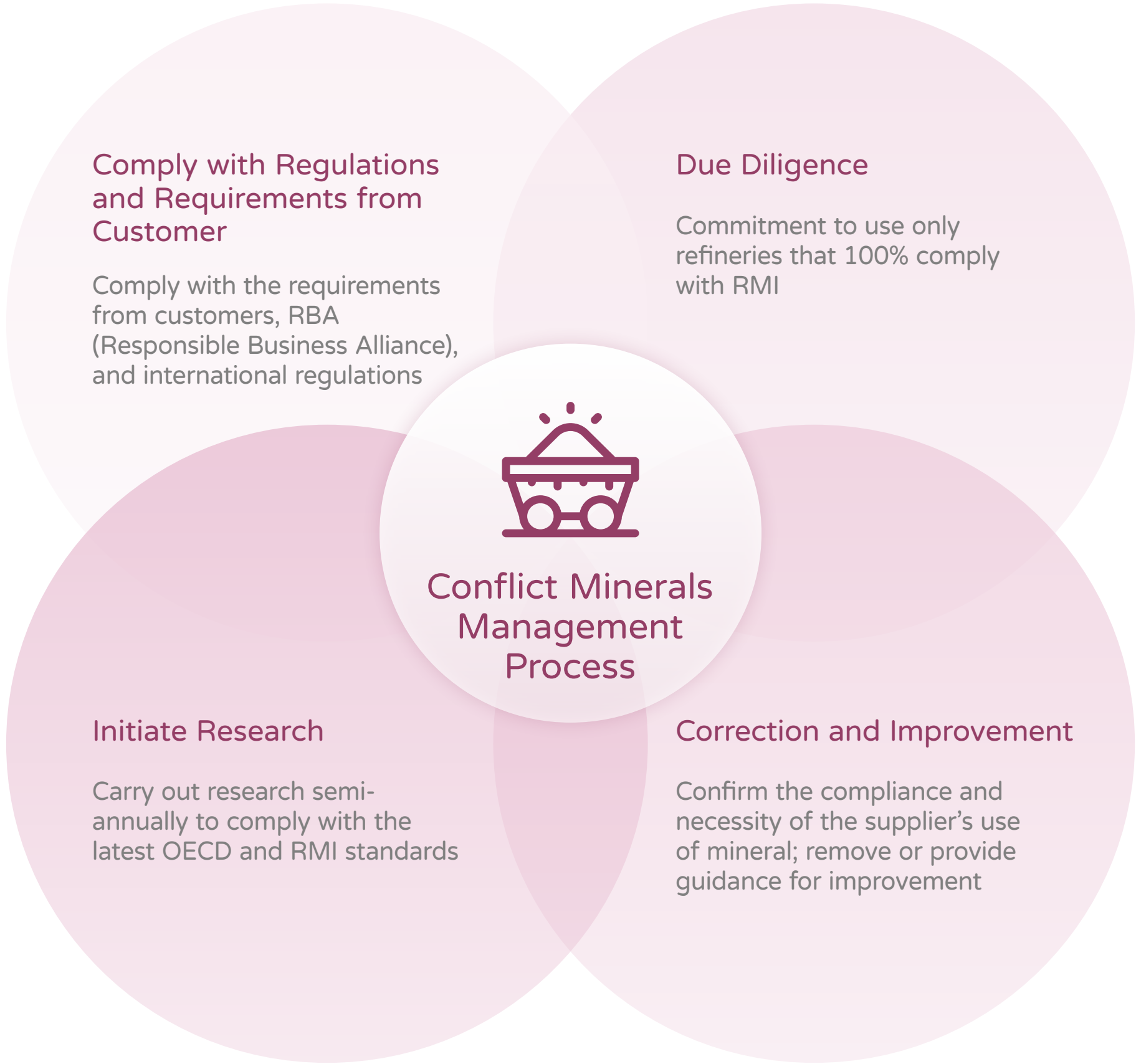
To achieve responsible and sustainable procurement practices, Wistron has established a conflict minerals policy and a responsible mineral sourcing management process. We are committed to sourcing minerals that adhere to the due diligence framework recognized by the Organization for Economic Co-operation and Development (OECD) in their "Due Diligence Guidance for Responsible Supply Chains of Minerals from Conflict-Affected and High-Risk Areas." We conduct thorough due diligence on our suppliers to ascertain which smelters and refiners possess systems that comply with prevailing global standards for responsible mineral sourcing. Furthermore, we prohibit the use of conflict minerals originating from high-risk regions.

Wistron adheres to the investigation findings of the Responsible Minerals Initiative (RMI) and has developed a "Conflict Minerals Management Procedure" to prevent the inadvertent acquisition of metals sourced from conflict minerals*. We explicitly mandate our suppliers to formulate policies ensuring the reasonable traceability of Gold (Au), Tantalum (Ta), Tungsten (W), Tin (Sn), Cobalt (Co), and Mica contained in our products, along with conducting due diligence to ensure their sources align with OECD requirements or have been excluded by organizations recognized for defining conflict-affected and high-risk areas for minerals.

Wistron conducts an annual reassessment of the smelters/refiners used in our products based on the Conformant Smelters List published on the RBA official website. We employ the Wistron SQP (Supplier Questionnaire Platform) questionnaire system and assessment to investigate conflict minerals systematically. Additionally, we utilize RMI's Conflict Minerals Reporting Template (CMRT) and Extended Minerals Reporting Template (EMRT) for investigations, requiring suppliers to disclose mineral sources and sign the Conflict Minerals Statement. This ensures that their procurement sources are not from conflict and high-risk areas and comply with customer and regulatory requirements. In 2024, a total of 1,326 suppliers signed the declaration, achieving a 100% compliance rate.

In our conflict minerals management process, we engage with suppliers to ascertain the reasons and necessity for using conflict minerals. If their usage is deemed non-essential, we request suppliers to discontinue the procurement and use of conflict minerals and to select new mineral sources. They must provide valid evidence that the new minerals comply with RBA requirements as conflict-free. If the usage of conflict minerals is deemed necessary, suppliers are requested to provide removal plans or improvement measures.

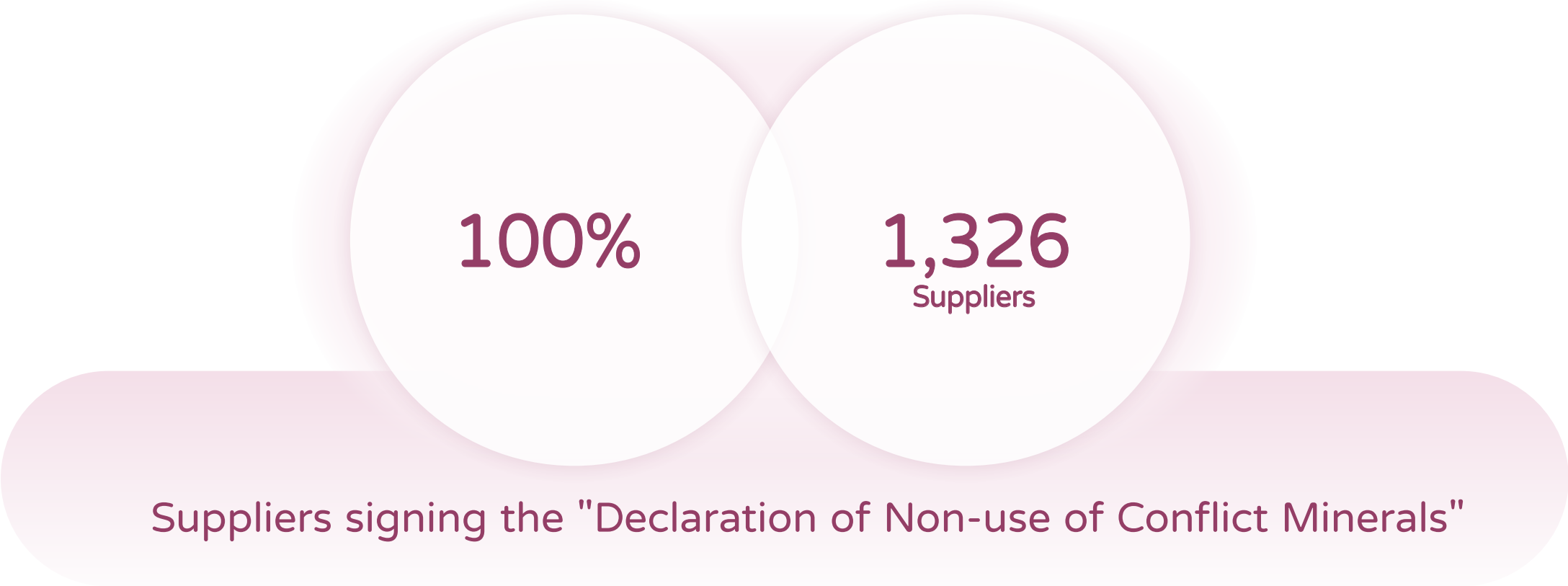
Since 2023, Wistron has begun affixing the declaration "CMRT-free" (Conflict Mineral-Free) on the outer packaging of our products, affirming that our company does not utilize conflict minerals. (The labeling may be adjusted according to different business units.)



Note : *Conflict Minerals are minerals extracted in conditions of armed conflict and human rights abuses. The main minerals subject to regulation include Gold (Au), Tantalum (Ta), Tungsten (W), Tin (Sn), Cobalt (Co), and Mica. These minerals are not only limited to the eastern provinces of the Democratic Republic of the Congo, which are controlled by the Congolese government forces and various armed rebel groups, but also extend to nine surrounding countries, including Angola, Burundi, the Central African Republic, the Republic of Congo, Uganda, Sudan, Tanzania, Rwanda, and Zambia, where the resources from these mines are extracted. Additionally, minerals from conflict-affected and high-risk areas, as defined by the OECD or an equivalent recognized organization, are also considered conflict minerals.



Signing of the “Declaration of Non-use of Conflict Minerals”



5.5 Operating Capability

5.5.1 Operational Achievements and Future Outlook

Wistron's consolidated revenue in 2024 was NT\$1.05 trillion. The net operating profit was NT\$3.9B. The net profit after tax was NT\$17.4B. The revenue and profit increased from 2023 and the net profit after tax reached a 10-year high.

In response to the increasingly intense industry competition, Wistron continues to strengthen its operational management by enhancing efficiency, advancing digital transformation, and driving innovation. The successful adoption of digital twin technology has enabled the development of future-ready factories, improving both production efficiency and product quality. Looking ahead, Wistron will continue to deepen its global presence, expand investments in high-tech innovations, and adjust its business models. At the same time, the company remains committed to ESG, leveraging innovation across multiple dimensions to achieve sustainable development goals and create long-term value for shareholders and society.

Financial Performance Indicators for the Past 4 Years

Unit: NT\$1M

Year / Item	2021	2022	2023	2024
Net revenues	862,083	984,619	867,057	1,049,256
Operating income	16,375	27,472	27,390	38,980
Net profit after tax	10,468	11,162	11,472	17,439

Note : Refer to the [Appendix 6.3](#) for the complete financial performance list

5.5.2 Tax Policy

Wistron’s Board of Directors is the highest decision-making and supervisory body for the Company’s taxation. It approves the [Tax Policy and Management Guidelines](#) as the foundation for the Company’s tax governance and adopts a reasonable tax management structure to ensure an appropriate tax burden in all key operating countries. This approach aims to support social and economic stability and promote the sustainable development of the Company’s operations.

Tax Information in the Past Two Years

Unit: NT\$1,000

Item	2023	2024	Average
Net profit before tax	24,320,694	39,975,476	32,148,085
Income tax expenses	6,055,409	9,339,245	7,697,327
Effective Income tax rate (%)	24.90	23.36	23.94
Income tax paid	11,011,697	5,559,333	8,285,515
Cash tax rate (%)	45.28	13.91	25.77

Note: Please refer to Wistron's 2024 Consolidated Financial Report for related information.

Income Tax Paid (Received) in Various Regions Between 2023 and 2024

Unit: NT\$1,000

Year	2023		2024	
	Amount	Percentage (%)	Amount	Percentage (%)
Asia	10,231,667	93	4,938,960	89
Americas	711,331	6	741,271	13
Europe	68,699	1	(120,898)	(2)
Total payment	11,011,697	100	5,559,333	100

5.5.3 Policy Influence

Wistron actively builds close collaborations with cross-industry and interdisciplinary groups and organizations, engaging deeply as a member to expand platforms for dialogue and broaden the scope of participation. Through collaboration with these organizations, Wistron stays informed of the latest international trends and developments, supporting the company’s ongoing growth and progress. In 2024, Wistron participated in the following organizations and associations:

Type	Organization or Trade association
Technology	<ul style="list-style-type: none"> Taiwan Electrical and Electronic Manufacturers’ Association Taipei Computer Association The Allied Association for Science Park Industries (ASIP) Nanotechnology and Micro System Association Taiwan Industry-Academia Research for Collaboration-Integration-Development Association
Medical	<ul style="list-style-type: none"> Taiwan Assistive Technology Industry Association Taiwan Medical and Biotech Industry Association
Others	<ul style="list-style-type: none"> Regular member of the Responsible Business Alliance (RBA) Member of the Gap of Learning & Field Member of the Commonwealth Sustainability League Member of the Business Council for Sustainable Development of the Republic of China (BCSD Taiwan)